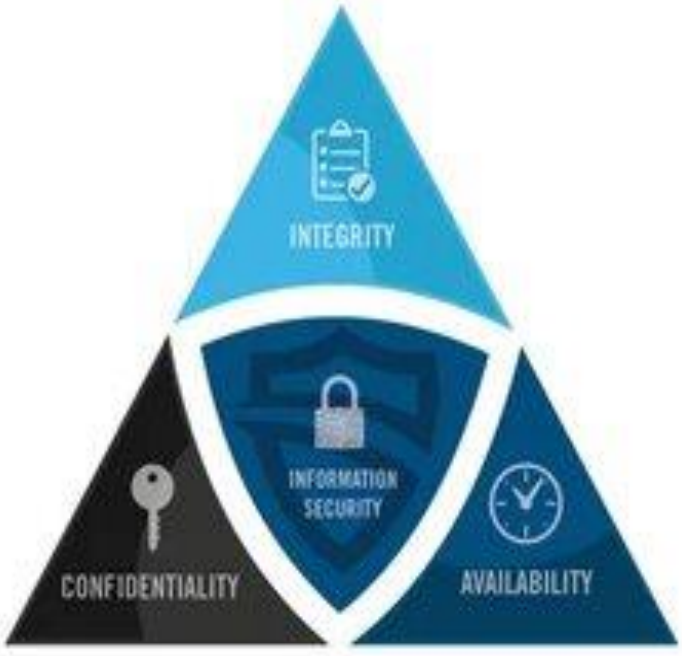
**МИНИСТЕРСТВО ЦИФРОВОГО РАЗВИТИЯ,
СВЯЗИ И МАССОВЫХ КОММУНИКАЦИЙ
РОССИЙСКОЙ ФЕДЕРАЦИИ**

ХИИК
СибГУТИ

**ХАБАРОВСКИЙ ИНСТИТУТ ИНФОКОММУНИКАЦИЙ (ФИЛИАЛ)
ФЕДЕРАЛЬНОЕ ГОСУДАРСТВЕННОЕ БЮДЖЕТНОЕ
ОБРАЗОВАТЕЛЬНОЕ УЧРЕЖДЕНИЕ ВЫСШЕГО ОБРАЗОВАНИЯ
«СИБИРСКИЙ ГОСУДАРСТВЕННЫЙ УНИВЕРСИТЕТ
ТЕЛЕКОММУНИКАЦИЙ И ИНФОРМАТИКИ»
ХИИК СибГУТИ**

ИНФОРМАЦИОННАЯ БЕЗОПАСНОСТЬ: ОБРАЗВАНИЕ. НАУКА. ОБЩЕСТВО.



(Монография, посвящена Десятилетию науки и технологий в России и празднованию 300-летия Российской академию наук)

**ХАБАРОВСК
2024**

УДК: 004 (063.330.341.1)
ББК: 99(225)-55я54

Издаётся согласно Планов научно-инновационной и редакционно-издательской деятельности ХИИК (филиал) ФГБО ВО СибГУТИ на 2024 год

Информационная безопасность: Образование. Наука. Общество. Монография посвящена Десятилетию науки и технологий в России и празднования 300-летия Российской академии наук / Под общ. ред.: Г.Ф. Маслова, Т.Е. Гварлиани, Р.М. Данилова, А.М. Межуева и др. – Хабаровск: Изд-во ХИИК (филиал) СибГУТИ, 2024. – 193 с.

РЕЦЕНЗЕНТЫ:

Кантышева А.В. – доцент, кандидат технических наук, доцент кафедры «ДВЮ МВД России», г. Хабаровск
Кононов Э.А. доцент, кандидат юридических наук, доцент кафедры ДВ филиал «РГУПС», х. Хабаровск
Кудряшов А.Б. – доцент, кандидат педагогических наук, доцент кафедры «ДВЮ МВД России», г. Хабаровск
Ярулин И.Ф. – профессор, доктор политических наук, ведущий научный сотрудник «ТОГУ», г. Хабаровск

Уважаемые коллеги, представленные Вашему вниманию материалы Межвузовского научного он-лайн семинара «Информационная безопасность: Образование. Наука. Общество», проведенного на базе Хабаровского института инфокоммуникаций (филиал) ФГБОУ ВО «Сибирский государственный университет телекоммуникаций и информатики» (18-19 января 2024 года) - это авторские исследования по актуальной тематике, включающее рассмотрение вопросов, касающихся аспектов информационной безопасности на современном этапе в образовании, экономике, праве, управлении и конечно в сфере разработки и использования IT-технологий.

Издание предназначено для практических работников IT-сферы, а также научному и научно-педагогическому составу научных и образовательных учреждений и конечно студентам и аспирантов проходящим обучение по направлению «Информационная безопасность».

ISBN 978-5-04-121144-4

© Авторский коллектив, 2024.
© Хабаровский институт инфокоммуникаций (филиал) ФГБОУ ВО «Сибирский государственный университет коммуникаций и информатики», 2024.

СОДЕРЖАНИЕ

ПЕРЕЧЕНЬ ОБРАЗОВАТЕЛЬНЫХ УЧРЕЖДЕНИЙ И НАУЧНЫХ ОРГАНИЗАЦИЙ ПРИНЯВШИХ УЧАСТИЕ В НАУЧНОМ СЕМИНАРЕ…… 5

Ярулин И.Ф. Вводная статья…… 10

ГЛАВА 1. Современные тенденции развития информационных технологий…… 13

1.1. *Обзор предложений на рынке защищенных операционных систем…….* 13

1.2. *Оптимизация расчётов транспортных SDH-сетей с использованием ячеек ПО «MS ExceL»……* 17

1.3. *Современные методы и технологии для организации безопасной работы в сети Интернет……* 24

1.4. *Искусственный интеллект в современном мире……* 30

1.5. *Способы оценки эффективности информационного обмена в цифровых системах связи с учетом информационных потерь……* 34

1.6. *Система управления обнаружением компьютерных атак на базе нейро-нечеткой логики в критической информационной инфраструктуре……* 45

1.7. *Онлайн компиляции кода агентов на платформе IACPAAS……* 47

1.8. *Прошлое и настоящее шифрования информации, в контексте обеспечения информационной безопасности……* 50

1.9. *Информационное и медиакоммуникационное обеспечение военной деятельности организации Североатлантического договора на современном этапе……* 55

1.10. *Методики разработки защиты информационных систем от DDOS-атак на основе применения алгоритмов роевого интеллекта….* 68

ГЛАВА 2. Проблемы информационной безопасности…… 71

2.1. *Анализ недостатков технологий обнаружения и расследования инцидентов безопасности……* 71

2.2. *К вопросу о обеспечении информационной безопасности государственных информационных ресурсов……* 77

2.3. *Анонимизация и деанонимизация пользователей интернет-порталов и социальных сетей в целях обеспечения информационной безопасности……* 82

2.4. *Телефонный терроризм, как форма проявления экстремизма……* 86

2.5. *Использование «электронной подписи» как способа защиты информации в сетях передачи данных ОВД России……* 93

2.6. *Современные тенденции развития информационных технологий по выявлению и предотвращению преступлений……* 99

2.7. *Основные направления информационной безопасности в условиях цифровизации*…….. 105
2.8. *Проблемы обеспечения информационной безопасности в Российской Федерации*…….. 110
2.9. *Противодействие Японии в информационно-психологической войне как составной части информационной безопасности России (на примере Сахалинской области)*…….. 112
2.10. *Вопросы повышения безопасности работы сотрудников пожарной охраны*…….. 121
2.11. *Информационно-психологическое противоборство: теоретико-практический аспект проблемы*…….. 126
2.12. *Кибербезопасность и внутренние и внешние угрозы, связанные с использованием компьютерных технологий*…….. 131
2.13. *Информационная безопасность как основное направление реализации национального проекта России «Цифровая экономика»*…… 134

ГЛАВА 3. Кадры для развития цифровизации…….. 137
3.1. *Подготовка кадров для развития цифровой экономики*…….. 137
3.2. *Разработка наборов базовых показателей для автоматизированной оценки «человеческого фактора» в сфере обеспечения информационной безопасности*…….. 144
3.3. *Подготовка кадров для IT-отрасли и конфликт интересов заказчиков и исполнителей*…….. 147
3.4. *Государственная система аттестации и лицензирования в сфере информационной безопасности*…….. 151
3.5. *Реализация технологий формирования субъектной позиции студентов в контексте обеспечения безопасности информации*…….. 155

ГЛАВА 4. Бизнес, экономика, управление в контексте обеспечения информационной безопасности…….. 161
4.1. *Анализ основных особенностей информационно-телекоммуникационных систем внутри производственных предприятий*…….. 161
4.2. *Перспективы применения цифровых технологий в организационных и функциональных механизмах экономической и правовой систем России в целях обеспечения информационной безопасности в условиях неопределенности*…….. 168
4.3. *Анализ оценки риска «утечек» конфиденциальных данных при удалённой работе В 2018-2020 годах*…….. 175
4.4. *Использование корпоративных информационных систем в контексте управления отраслевой информационной безопасностью на предприятиях индустрии туризма и гостеприимства*…….. 179

СВЕДЕНИЯ О АВТОРАХ…… 189

ПЕРЕЧЕНЬ
образовательных учреждений и научных организаций, принявших участие в научном семинаре

НАУЧНЫЕ ОРГАНИЗАЦИИ

АНО «ЦИМО АТР»

Автономная некоммерческая организация «Центр изучения международных отношений в Азиатско-Тихоокеанском регионе»
(г. Хабаровск, Россия)

ИАПУ ДВО РАН

«Институт автоматики и процессов управления» Федеральное государственное бюджетное учреждение науки «Дальневосточное отделение Российской академии наук»
(г. Владивосток, Россия)

Университет 20.35

Автономная некоммерческая организация «Университет национальной технологической инициативы 20.35»
(г. Москва, Россия)

ОБРАЗОВАТЕЛЬНЫЕ УЧРЕЖДЕНИЯ

АНОО ВО «ВИВТ»

Автономная некоммерческая организация высшего образования «Воронежский институт высоких технологий»
(г. Воронеж, Россия)

БелЮИ МВД РФ имени И.Д. Путилина

Федеральное государственное казенное образовательное учреждение высшего образования МВД России «Белгородский юридический институт Министерства внутренних дел Российской Федерации имени И.Д. Путилина»
(г. Белгород, Россия)

БИИК «СибГУТИ		*Бурятский институт инфокоммуникаций (филиал) Федерального государственного образовательного учреждения высшего образования «Сибирский государственный университет телекоммуникаций и информатики» (г. Улан-Удэ, Республика Бурятия, Россия)*
ВГЛУ им. Г.Ф. Морозова		*Федеральное государственное образовательное учреждение высшего образования «Воронежский государственный лесотехнический университет имени Г.Ф. Морозова» (г. Воронеж, Россия)*
ВГУ		*Федеральное государственное бюджетное образовательное учреждение высшего образования «Воронежский государственный университет» (г. Воронеж, Россия)*
ВИ МВД России		*Федеральное государственное казенное образовательное учреждение высшего профессионального образования МВД России «Воронежский институт Министерства внутренних дел Российской Федерации» (г. Воронеж, Россия)*
ВИ ФСИН России		*Федеральное казенное образовательное учреждение высшего образования «Воронежский институт Федеральной службы исполнения наказаний Российской Федерации» (г. Воронеж, Россия)*

ВолИУ филиал «РАНХиГС»		*Волгоградский институт управления - филиал Федерального государственного бюджетного образовательного учреждения высшего образования «Российская академия народного хозяйства и государственной службы при Президенте Российской Федерации» (г. Волгоград, Россия)*
ВУНЦ ВВС «ВВА им. профессора Н.Е. Жуковского и Ю.А. Гагарина»		*Федеральное государственное казённое военное образовательное учреждение высшего профессионального образования Военный учебно-научный центр Военно-воздушных сил «Военно-воздушная орденов Ленина и Октябрьской Революции, дважды Краснознамённая, орденов Кутузова и Жукова академия имени профессора Н.Е. Жуковского и Ю.А. Гагарина» Министерства обороны Российской Федерации (г. Воронеж, Россия)*
ДВГУПС		*Федеральное государственное образовательное учреждение высшего образования «Дальневосточный государственный университет путей сообщения» (г. Хабаровск, Россия)*
ДВИ (филиал) «ВГУЮ (РПА Минюста России)»		*Дальневосточный институт (филиал) Федерального государственного бюджетного образовательного учреждения высшего образования «Всероссийский государственный университет юстиции (Российская правовое академия Министерства юстиции Российской Федерации)» (г. Хабаровск, Россия)*
ДВИУ – филиал РАНХиГС		*Дальневосточный институт управления – филиал Федерального государственного бюджетное образовательное учреждение высшего образования «Российская академия народного хозяйства и государственной службы при президенте Российской Федерации» (г. Хабаровск, Россия)*

ДВЮИ МВД России

Федеральное государственное казенное образовательное учреждение высшего профессионального образования МВД России «Дальневосточный юридический институт Министерства внутренних дел Российской Федерации» (г. Хабаровск, Россия)

МосУ МВД России имени В.Я. Кикотя

Федеральное государственное казенное образовательное учреждение высшего профессионального образования МВД России «Московский юридический университет Министерства внутренних дел Российской Федерации имени В.Я. Кикотя» (г. Москва, Россия)

МТУСИ

Ордена Трудового Красного Знамение федеральное государственное образовательное учреждение высшего образования «Московский технический университет связи и информатики» (г. Москва, Россия)

ПГУТИ

Федеральное государственное образовательное учреждение высшего образования «Приволжский государственный университет телекоммуникаций и информатики» (г. Самара, Россия)

СГУ

Федеральное государственное автономное образовательное учреждение высшего образования «Сочинский государственный университет» (г. Сочи, Россия)

СКФУ		*Федеральное государственное автономное образовательное учреждение высшего образования «Северо-Кавказский федеральный университет» (г. Ставрополь, Россия)*
СПбПУ Петра Великого		*Федеральное государственное автономное образовательное учреждение высшего образования «Санкт-Петербургский политехнический университет Петра Великого» (г. Санкт-Петербург, Россия)*
СФУ		*Федеральное государственное автономное образовательное учреждение высшего образования «Сибирский федеральный университет» (г. Красноярск, Россия)*
ТОГУ		*Федеральное государственное образовательное учреждение высшего образования «Тихоокеанский государственный университет» (г. Хабаровск, Россия)*
ХИИК «СибГУТИ»		*Хабаровский институт инфокоммуникаций (филиал) Федерального государственного образовательного учреждения высшего образования «Сибирский государственный университет телекоммуникаций и информатики» (г. Хабаровск, Россия)*

Информационная безопасность Российской Федерации - состояние защищенности личности, общества и государства от внутренних и внешних информационных угроз, при котором обеспечиваются реализация конституционных прав и свобод человека и гражданина, достойные качество и уровень жизни граждан, суверенитет, территориальная целостность и устойчивое социально-экономическое развитие Российской Федерации, оборона и безопасность государства

Ч 1, ст. 2, п. В. Доктрина информационной безопасности Российской Федерации. Утвержденная Указом Президента Российской Федерации от 5 декабря 2016. № 646

Доминирующей тенденцией развития современной цивилизации в XXI веке является новая информационно-технологическая революция, которая уже охватила многие страны мирового сообщества. Ее отличительной особенностью становится стремительное развитие новых информационных и коммуникационных технологий и их проникновение практически во все сферы жизнедеятельности общества. Эти технологии быстро становятся атрибутом современной культуры. Они существенным образом изменяют образ и качество жизни миллионов людей, формируют у них новые стереотипы поведения и общения, а также новые привычки и ценности.

Стремительное развитие цифровых технологий приводит к кардинальным изменениям привычного уклада жизни человека и с каждым годом влияние новых технологий усиливается. В связи с этим возрастает количество этических и других вопросов, которые требуют их осмысления. Сегодня не является секретом имеющая место быть глубокая зависимость безопасного мира от условий развития и уровня безопасности информационной среды общества. Именно через информационную среду осуществляются главные угрозы жизненно важным интересам не только граждан, но и государств, и как следствие этого наблюдается рост информационной составляющей во всех видах национальной безопасности.

Развитие технологий создает определенные риски в виде усиления неравенства, риска утечки личных данных человека, трансформации рынка труда и потери частью населения рабочих мест, изменений социальных отношений и т.д. Происходит значительное развитие и усложнение роли информационной безопасности в обществе.

Одновременно с негативными явлениями, современные технологии формируют новые потенциалы для различных групп населения, открывая возможности дистанционного обучения, онлайн-покупок, мобильных банков, новых методов обеспечения безопасности и т.д. Успешное внедрение этих технологий в деятельность человека зависит от отношения населения к инновациям, от готовности к переменам. Безусловно, общество пугает все новое и неопределенное, поэтому выведение в публичное поле дискуссии о произошедших и ожидаемых переменах в образе жизни населения в процессе цифровизации является необходимым шагом.

Одной из наиболее актуальных проблем является проблемы практической реализации потенциальных возможностей информационной безопасности различных социальных систем для обеспечения их нормальной деятельности и интеграции в

мировую систему. Наличие данной проблемы во многом обусловлено имеющимися противоречиями в вопросах изучения, обобщения и распространения практики формирования систем информационной безопасности.

Указом Президента Российской Федерации от 9 мая 2017 года утверждена новая «Стратегия развития информационного общества в Российской Федерации на 2017-2030 годы»[1] (далее – «Стратегия»), которая определила цели, задачи и меры по реализации внутренней и внешней политики России в сфере применения информационных и коммуникационных технологий. «Стратегия» определяет, что обеспечение национальных интересов осуществляется посредством реализации приоритетов в условиях развития информационного общества. Для точного понимания стратегии по развитию информационного общества Российской Федерации, необходим анализ объявленных в документе стратегических приоритетов и принципов.

Ключевым элементом в определении направлений и содержания принятия управленческих решений в рассматриваемой сфере является «Доктрина информационной безопасности Российской Феде-рации» в ее действующей редакции, которая представляет собой: «систему официальных взглядов на обеспечение национальной безопасности Российской Федерации в информационной сфере»[2].

Из перечисляемых угроз в сфере информационной безопасности России особое внимание следует обратить на угрозы информационному обеспечению государственной политики Российской Федерации. Согласно доктринальному документу, в данной сфере выделяются следующие основные угрозы:

- неконтролируемый трансграничный рынок оборота информации, который отдельные акторы международной системы могут использовать, в том числе и для реализации своих агрессивных геополитических целей;

- специальные службы ряда государств разработали средства нформационно-психологического воздействия по дестабилизации социально-политической ситуации в целях подрыва суверенитета и территориальной целостности других стран;

- зарубежные государства наращивают усилия по информационно-агитационной работе с российским населением (в первую очередь с молодежью) в целях подрыва традиционных духовных ценностей России;

- террористические организации овладели современными информационными технологиями по продвижению экстремистских идеологий в политическое сознание социальных групп, отдельных граждан;

- кадровое и технологическое отставание России от ведущих государств в сфере информационной безопасности[3].

Масштабная цифровизация оказывает непосредственное влияние не только на повседневную жизнь граждан, она, естественно, вносит нестабильность и турбулентность в сегодняшний политический процесс, особенно в разные технологии легитимации политических режимов. Модераторы популярных сетевых сообществ, политически мотивированные хакеры, глобальные цифровые компании, экстремистские сетевые группы, интересанты сетевых движений, развитые в информационно-коммуникационном плане государства – это далеко не полный перечень тех акторов, которые начинают вмешиваться в ранее налаженные и закрепленные политической властью легитимационные приемы.

---

[1] Российская Федерация. Указы. Стратегия развития информационного общества в Российской Федерации на 2017-2030 годы. Утверждена Указом [Путин В.В.] Президента Российской Федерации от 9 мая 2017 № 203 // СПС «KREMLIN.ru»

[2] Российская Федерация. Указы. Доктрина информационной безопасности Российской Федерации. Указ Президента [Путин В.В.] Российской Федерации от 5 декабря 2016 № 646 // СПС «GARANT.ru».

[3] Там же.

В политической, деловой, научной и образовательной сферах общества также происходят радикальные трансформации, которые сопровождаются возникновением новых профессий, научных и образовательных дисциплин, способов общения между людьми в их совместной деятельности. При этом в последние годы появляется все больше новых понятий и терминов, содержание которых требует адекватного понимания.

В системе государственного управления России мы имеем дело со сложной проблемой научно-практического характера – поиск путей оптимизации государственной политики по обеспечению информационной безопасности страны, органов государственной власти, институтов гражданского общества, интересов личности. Решение данной проблемы неразрывно связано с разработкой эффективных механизмов обеспечения легитимации деятельности государственных институтов России, что является залогом стабильности политической системы в целом.

Необходимость всесторонних исследований в сфере государственного управления сферой информационной безопасности не утратила своей актуальности и в текущий момент, поскольку особенности экономических, политических, культурно-цивилизационных процессов в глобальном масштабе генерируют в отношении России новые вызовы и угрозы в информационной сфере, нуждающиеся в своевременном изучении и разработке способов защиты от них.

В предлагаемом читателям сборнике материалов коллективной монографии предпринята попытка решения проблемы информационной безопасности путем раскрытия и обсуждения содержания ряда новых подходов и практик, которые сегодня используются в данной области. Многие из них являются новыми, они появились в последние годы и поэтому еще не представлены в существующей научной литературе.
Особо хотелось бы отметить актуальность этой проблемы для преподавателей и студентов системы высшего и среднего образования России, которая сегодня приступила к реализации новой стратегии своего инновационного развития на основе глубокой и широкомасштабной цифровой трансформации общества. Указом Президента России «О национальных целях развития Российской Федерации на период до 2030 года» цифровая трансформация объявлена одной из пяти национальных целей нашей страны на этот период. При этом предполагается, что достижение этой цели обеспечит успешное достижение других национальных целей России, из которых наиболее приоритетной является «сохранение населения, здоровье и благосостояние людей»[4].

Структура сборника определена целью, задачами исследования. Даются четкие, понятные формулировки. Предложенные положения не содержат противоречий, имеют прямое отношение к авторским методологическим, аналитическим приемам, способам концептуализации. Стиль работы вполне академичен и соответствует требованиям к научным работам такого формата.

Надеемся, что материалы сборника послужат дальнейшему решению проблем информационной безопасности всех сфер жизнедеятельности Российской Федерации.

Ярулин Илдус Файзрахманович,
доктор политических наук, профессор
научный руководитель Института социально-политических технологий и коммуникаций ФГБОУ ВО «Тихоокеанский государственный университет»

[4] Российская Федерация. Указы. О национальных целях развития Российской Федерации на период до 2030 года. Указ Президента [Путин В.В.] Российской Федерации от 21 июля 2020 № 474 // СПС «KREMLIN.ru»

ГЛАВА 1.
СОВРЕМЕННЫЕ ТЕНДЕНЦИИ РАЗВИТИЯ ИНФОРМАЦИОННЫХ ТЕХНОЛОГИЙ

1.1. ОБЗОР ПРЕДЛОЖЕНИЙ НА РЫНКЕ ЗАЩИЩЕННЫХ ОПЕРАЦИОННЫХ СИСТЕМ

В представленной автором работе рассматриваются популярные операционные системы (ОС), позиционирующие себя как защищенные и анонимные, угрозы от которых защищают такие системы, а также основные законы, регулирующие работу с ЭВМ и деятельность в интернете. Как итог – определено направление дальнейшего исследования.
Ключевые слова: информация, информационная безопасность (ИБ), защищенные операционные системы, кибербезопасность, программное обеспечение (ПО).

OVERVIEW OF OFFERS ON THE SECURED OPERATING SYSTEMS MARKET

The work presented by the author examines popular operating systems (OS), positioning themselves as secure and anonymous, threats from which such systems protect, as well as the basic laws governing work with computers and activities on the Internet. As a result, the direction for further research has been determined.
Keywords: information, information security (IS), secure operating systems, cybersecurity, software.

В современном мире почти у каждого есть электронный гаджет: системный блок, смартфон, моноблок, ноутбук и другие, а у большинства людей по несколько. Всем этим устройствам приходится постоянно обрабатывать информацию и взаимодействовать друг с другом через интернет.

Сейчас можно в любой момент связаться родными, коллегами, друзьями, позвонить или написать, поделиться веселой картинкой или роликом, переслать или скачать документы и файлы, никто не будет спорить, что это очень удобно и значительно облегчает жизнь.

Всегда были люди, стремящиеся получить выгоду из чужого горя. Если раньше, в до «цифровую эпоху» можно было сразу определить, от кого исходит угроза, то сейчас все больше злоумышленников маскируются в сети под безобидных личностей или используют чужие. Темные хакеры постоянно создают все новые возможности для обогащения. Они могут украсть данные жертвы, следить за ней, шантажировать, использовать устройство в своих целях без ведома владельца (например, для DDoS атак), временно украсть аккаунт от почты или в соцсети, чтобы от вашего лица делать какие-то действия и многое другое. К сожалению, никто от этого не застрахован, но возможно снизить риски этих событий.

Существует ряд компьютерных уязвимостей, причиной которых зачастую является недосмотр программиста. На эти уязвимости совершаются атаки. Суть атаки может быть разная, но ее однозначно нельзя назвать успешной, если злоумышленник не смог получить какие-либо важные данные, или закрепиться в сети (на устройстве).

Можно выделить следующие виды вредоносного ПО (malware), которыми пытаются заразить устройства:

1. Бэкдоры (back door*). По сути бэкдор – это своеобразная лазейка, зная которую, можно проникнуть в систему, однако, сам по себе он ничего не делает, а служит лишь точкой входа. Их особенность в том, что они могут создаваться как blackhat хакерами, так и закладываться преднамеренно разработчиками ПО*.

2. Черви. *Их главная особенность в том, что они работают без участия человека, самостоятельно распространяясь по сети и/или через подключаемые устройства и выполняя заложенные функции. С их помощью могут формироваться ботнэты (botnet) используемые для различных атак, например DDoS, или целевых*

фишинговых атак (spear phishing), при этом работая полностью в автоматическом режиме.

3. Руткиты (rootkit). *Данный тип вируса опасен тем, что встраивается в ядро системы, из-за чего, обладает самыми высокими привилегиями и при этом остается не замеченным, для антивирусного ПО. Важно понимать, что сам руткит может никак не проявлять себя в системе, а например, просто собирать данные пользователя, такие как: персональная информация, пароли, паспортные данные, номера кредитных и дебетовых карт и прочее, что может хранится на компьютере.*

3. Шифровальщики. *Шифруют системы и требуют выкуп для разблокировки. Однако зачастую ни злоумышленники, ни даже сама программа не знает пароль, которым шифровалось система и дальнейшее восстановление данных становиться большим вопросом.*

Вирусы используют одни и те же механизмы для внедрения и работы, существующие уже много лет. Они могут быть связанны с распределением программы в памяти, например переполнение буфера или висячий указатель, когда идет попытка подмены адреса, в оперативной памяти, который ведет на вредоносный код. Или с особенностью выполнения программы, например разного рода кодов типа «Injection» (инъекция), «SQL», «PHP», «JavaScript», «Email» и другие, когда использую особенности обработки запросов и работы самого сервиса, чтобы вызвать поведение, отличное от обычного.

Так или иначе любое ПО в том числе и вирусное взаимодействуют с ОС, именно от ее работы и настройки зависит, как много проблем они могут доставить, хотя осведомленность пользователя в этом вопросе и принимаемые действия не менее важны.

Создание любой защиты и соблюдение определенных правил, для ее сохранения требуют ресурсов, и чем выше степень защити, тем больше их требуется. Таким образом, меры по обеспечению информационной безопасности требуются только в случае, если мы имеем дело с тайной.

Тайна – это какая-либо информация, которая должна быть известна только определенному кругу лиц и/или в случае ее огласки могут наступить негативные последствия для владельца, моральный или материальный ущерб.

Самым главным документом в Российской Федерация (РФ, Россия), регулирующим остальные правовые нормы, является Конституция России. Согласно статье 23 каждый имеет право на неприкосновенность частной жизни, личную и семейную тайну, а также право на тайну переписки, телефонных переговоров, почтовых телеграфных и иных сообщений. Согласно статье 24 «… сбор, хранение, использование и распространение информации о частной жизни лица без его согласия не допускается». [3].

Существует так же ряд других кодексов, законов, указов, постановлений и приказов относящиеся к защите и распространению информации. В работах: «Правовое регулирование защиты информации в государственных информационных системах» под авторством Филипповой Н.В. и «Защита конфиденциальности информации в гражданском процессе» [16] авторов Лошкаревой А.В., Фадеевой А.В. и Трошенковой А.И.[4], рассматриваются часть федеральных законов, документов ФСТЭК, постановления правительства и другое, касающееся правовых аспектов защиты информации, дополняющих рассмотренные выше.

Операционная система (ОС) – программное обеспечение, управляющее аппаратным обеспечением, предоставляющее абстрактный программный интерфейс для взаимодействия с ним и занимающееся распределением предоставляемых ресурсов, в том числе между прикладными программами. [8]. Любая ОС обязательно включает три элемента: планировщик задач, модуль управление памятью и наблюдение за обменом данными между потоками, одного или разных, процессов.

В большинстве современных ОС встроены базовые механизмы защиты как в «Windows» [1], так и в «Linux» [5]. Однако не всем их достаточно, к тому же некоторые ОС имеют закрытый исходный код, что не позволяет в достаточной мере проконтролировать ее выполнение.

Для таких случаев разрабатываются защищенные ОС. Они имеют более расширенный пакет программ и механизмов, дополнительно, защищающих информацию от кражи или потери. Для России перечни таких механизмов перечислены в документах ФСТЭК [7].

Из ОС, позиционирующих себя как защищенные и анонимные, можно выделить следующие «QubesOS», «OpenBSD» и «Whonix». Каждая из них разрабатывается сообществом, а исходный код открыт.

«QubesOS» позиционируется как самая защищенная и анонимная ОС, с открытым исходным кодом, которая есть на рынке. В своей работе она активно использует виртуальные контейнеры (кубы), основанные на гипервизоре первого типа «Xen». Каждая программа запускается в отдельно выбранном контейнере, которые изначально никак не связанны между собой, что значительно повышает безопасность. Например, ведь можно выходить в интернет через один куб, а работать в другом, который вообще не связан с другими кубами. Однако за такие особенности приходится платить. Эта ОС очень требовательна к комплектующим и комфортно использовать ее на старом или маломощном компьютере будет проблематично.

«Whonix» предназначена в основном для анонимной работы в интернете. Анонимность создается за счет того, что весь выходной трафик оборачивает в сеть «Tor». Этот дистрибутив не годится для полноценной замены «Debian» или «Arch», из-за своей специфики и используется он, в основном как дополнение к основной ОС.

«OpenBSD» в силу своей архитектуры можно считается очень безопасной. К сожалению, из-за особенностей разработки BSD систем, когда каждый разработчик работает над своей собственной ОС включая ядро, возникают некоторые недостатки. Стоит отметить, что BSD системах используются другие консольные команды для общения с системой, по сравнению с «Linux», хотя они и могут иметь похожий синтаксис. Так же отсутствуют, даже аналоги, некоторых привычных «Linux»-команд. Вдобавок эта система несовместима с некоторыми устройствами, например ноутбуками и видеокартами. Эта система великолепно подойдет для серверов, где часто и применяется из-за высокой стойкости к атакам и малого количества уязвимостей. Для рядового пользователя, для дома, эта система будет крайне неудобна из-за скудности функционала и сложности эксплуатации. А вот для работы с важными данными, где-нибудь на производстве или в качестве сервера вполне может подойти.

Связи с уходом из РФ некоторых иностранных компаний [15] возникает необходимость в разработке продуктов, в первую очередь ориентированных, на внутренний рынок.

Уже готовую защищенную ОС «Astra Linux», предлагают российские разработчики. Она основана на дистрибутиве «Debian» и официально является одной из веток (fork). «Astra Linux Common Edition» является операционной системой общего назначения. В ней не такая продвинутая защита, что повышает совместимость со сторонними программами и удобство использования, особенно это важно для домашних пользователей, которые хотят дополнительно обезопасить себя, но при этом не готовы изучать технический вопрос.

Так же в линейке продуктов есть «Astra Linux Special Edition», которая соответствует всем стандартам безопасности и может использоваться для обработки данных, составляющих государственную тайну, в том числе с грифом «особой важности».

«KasperskyOS», это собственная и независимая разработка «Лаборатории Касперского». Сами создатели утверждают, что это не совсем ОС, а микроядро [9]. Оно

состоит всего из десятков тысяч строк, в то время как другие ОС содержат миллионы строк, что в теории заметно повышает защищенность системы.

Некоторые специалисты считают, что на каждые 5000-10000 строк кода находится одна уязвимость, это очень условные данные, но суть отражают верно – чем больше кода, тем больше потенциальных уязвимостей. Например, современное ядро «Linux» содержит более 24 миллионов строк кода; «Debian» около 55; OpenBSD - 2.9. Если верить этим цифрам, то современные ОС содержат тысячи уязвимостей, однако не все они найдены и не все активно используются злоумышленниками, чтобы привлечь внимание для решения.

«Эльбрус» ОС с открытым исходным кодом, разрабатывается в России, компанией МЦСТ. Существуют версии для процессоров архитектуры x86 и отечественной разработки «Эльбрус». Основана на «Debian». «Эльбрус» ОС использует свою собственную систему сборки пакетов, причем сами пакеты весят и вмещают больше информации и равносильны 5-20 пакетам в других дистрибутивах. В системе не так много программ, к тому же они достаточно старые, в целом этого недостаточно для полноценной работы, но при необходимости можно установить дополнительное и более свежее ПО, т.к. система использует deb-пакеты.

В данной работе были рассмотрены наиболее популярные защищенные операционные системы, как зарубежные, так и российские разработки, существуют и другие ОС, но они не так популярны. Как видим на рынке достаточно предложений разного уровня доступности и функциональности. Любой может найти для себя наиболее подходящую систему исходя из целей.

Однако, можно ли создать операционную систему, с высоким уровнем защищенности, с помощью общедоступных программ с открытым исходным кодом, при том доступную для использования не только профессионалам, но и обычным пользователям, не особо разбирающимися в компьютерах? В этом и состоит суть будущего исследования.

Перечень использованной литературы и источников:

1. Безопасность операционной системы Windows-Microsoft. [Электронный ресурс]. – URL: https: learn.microsoft.com/ru-ru/windows/security/operating-system (Дата обращения: 01.04.2023).
2. Информационное сообщение ФСТЭК России от 18 октября 2016 г. N 240/24/4893 – ФСТЭК России [Электронный ресурс]. – URL: https://fstec.ru/normotvorcheskaya/informatsionnye-i-analiticheskie-materialy/1206-informatsionnoe-soobshchenie-fstek-rossii-ot-18-oktyabrya-2016-g-n-240-24-4893 (Дата обращения: 01.12.2023).
3. Конституция Российской Федерации (с Гимном России). – Москва: Проспект, 2020. – 64с.
4. Лошкарева А.В. Защита конфиденциальной информации в гражданском процессе / А.В. Лошкарева, А.В. Фадеева, А.И. Трошенкова // Modern Sciense. – 2019. – С. 257-261.
5. Механизмы безопасности в Linux – Хабр [Электронный ресурс]. – URL: https://habr.com/ru/post/92239/ (Дата обращения: 01.12.2023)
6. Н.С. Кармановский. Организационно-правовое и методическое обеспечение информационной безопасности: учебное пособие / Н.С. Кармановский, О.В. Михайличенко, С.В. Савков. – СПб.: Университет ИТМО, 2013. – 148 с.
7. Нормативные правовые акты, организационно-распорядительные документы, нормативные и методические документы и подготовленные проекты документов по технической защите информации – ФСТЭК России. [Электронный ресурс]. – URL: https://fstec.ru/normotvorcheskaya/tekhnicheskaya-zashchita-informatsii (Дата обращения: 01.12.2023)
8. Операционная система – Википедия. [Электронный ресурс]. – URL: https://ru.wikipedia.org/wiki (Дата обращения: 10.12.2023)
9. Основа кибериммунной операционной системы – kaspersky.ru. [Электронный ресурс]. – URL: https://os.kaspersky.ru/technologies/microkernel/ (Дата обращения: 10.12.2023).
10. Приказ ФСТЭК России от 18 февраля 2013 № 21. [Электронный ресурс]. – URL: https://fstec.ru/normotvorcheskaya/akty/53-prikazy/691-prikaz-fstek-rossii-ot-18-fevralya-2013-g-n-21 (Дата обращения: 10.12.2023).
11. Специальные нормативные документы ФСТЭК. [Электронный ресурс]. – URL: https://fstec.ru/tekhnicheskaya-zashchita-informatsii/dokumenty/114-spetsialnye-normativnye-dokumenty (Дата обращение 10.12.2023).

12. Суханов В.В. Аналитическое обеспечение организации данных в распределенных информационных системах критического применения / В.В. Суханов // Моделирование систем и процессов. – 2021. - Т. 14, № 3. – С. 60-67.
13. Суханов В.В. Методика логического проектирования информационного обеспечения распределенных информационных систем критического применения / В.В. Суханов, О.В. Ланкин // Моделирование систем и процессов. – 2021. - Т. 14, No 3. – С. 67-73.
14. Уголовный кодекс РФ // СПС «КонсультантПлюс».
15. Ушел и не вернулся: какие ИТ-компании покинули Россию, и кто сможет занять их место – Generation. [Электронный ресурс]. – URL: https://generation-startup.ru/media-center/smi/68551/ (Дата обращения: 10.12.2023)
16. Филипова Н.В. Правовое регулирование защиты информации в государственных информационных системах / Н.В. Филипова // Охрана. Безопасность. Связь- 2021. – С. 73-78. (ВИ МВД России).
17. Хрящев В.В. Эффективность внедрения одноранговой распределенной системы хранения и обработки защищаемой информации (TheOoL Project) / В.В. Хрящев, А.В. Ненашев // Моделирование систем и процессов. – 2021. – Т. 14, №3. – С. 82-89.
18. Заревич А.И., Макаренко Ф.В., Ягодкин А.С., Зольников К.В. Моделирование поведения мобильных роботов с использованием генетических алгоритмов // Моделирование систем и процессов. – 2022. - Т. 15, № 3. – С. 7-16.
19. Зольников В.К., Гамзатов Н.Г., Анциферова В.И., Полуэктов А.В., Фиронов В.А. Экспериментальные исследования радиационного воздействия на микросхемы FRAM // Моделирование систем и процессов. – 2022. - Т. 15, № 3. – С. 16-24.

1.2. ОПТИМИЗАЦИЯ РАСЧЁТОВ ТРАНСПОРТНЫХ SDH-СЕТЕЙ С ИСПОЛЬЗОВАНИЕМ ЯЧЕЕК ПО «MS EXCEL»

Для организации информационного обмена между отдельными локальными и глобальными сетями развертывается транспортная сеть (ТС), реализующая сервисы транспортировки информационных потоков между отдельными абонентами, а также предоставление информационных сервисов (таких как: радио, ТВ, факсимильная связь и др.) потребителям. И, поэтому в данной статье рассмотрен процесс оптимизации проведения расчётов SDH-сетей, с применением универсальных формул в ячейках ПО «MS Excel» - как одно из средств улучшения сервиса, но защиты его от несанкционированного «вторжения».
Ключевые слова: защита информации, информация, канал тональной частоты, необслуживаемый регенерационный пункт, оптимизация ПО «MS Excel», основной цифровой канал, плезиохронная цифровая иерархия, регенерационный участок, синхронная цифровая иерархия, транспортные сети (ТС), цифровая транспортная структура (ЦТС).

OPTIMIZATION OF TRANSPORTATION CALCULATIONS SDH NETWORKS USING MS EXCEL CELLS

To organize information exchange between individual local and global networks, a transport network (TC) is being deployed, which implements services for transporting information flows between individual subscribers, as well as providing information services (such as radio, TV, fax, etc.) to consumers. And, therefore, this article discusses the process of optimizing the calculations of SDH networks, using universal formulas in MS Excel cells - as one of the means to improve the service, but protect it from unauthorized "intrusion".
Keywords: information protection, information, tonal frequency channel, unattended regeneration point, MS Excel optimization, main digital channel, plesiochronous digital hierarchy, regeneration site, synchronous digital hierarchy, transport networks (TS), digital transport structure (DTS).

Транспортная сеть (ТС) – это совокупность ресурсов, выполняющих функции транспортирования в телекоммуникационных сетях [1]. Она включает не только системы передачи, но и относящиеся к ним средства контроля, оперативного переключения, резервирования, управления и защиты.

Необходимость защиты информации в ТС возникает по следующим основным причинам [2,6,7]:

- защита файла и его содержимого от случайной модификации, которую не всегда легко заметить и которая исказит используемые данные;

- защита конфиденциальной информации от лиц, не имеющих права доступа к ней.

Современной технологией для ТС, в настоящее время, является синхронная цифровая иерархия («Synchronous Digital Hierarchy» (SDH), так как в отличие от плезиохронной цифровой иерархии («Plesiochronous Digital Hierarchy» (PDH) имеет ряд преимуществ.

SDH – это цифровая транспортная структура (ЦТС), предназначенная для переноса по физической сети адаптированной нагрузки в виде STM и имеющая строго регламентированные интерфейсы узлов сети [4,5].

Недостатки PDH:

- Наличие сразу несколько иерархий;
- Характер мультиплексирования обуславливается трудностью ввода и вывода каналов в промежуточных пунктах;
- Отсутствие возможности организации дополнительных каналов, что в результате почти полностью отсутствуют средства сетевого автоматизированного контроля и управления, а без этой возможности нельзя создать надёжную сеть связи с высоким качеством обслуживания.

Достоинства SDH [4,5]:

- Современная компонентная база;
- Большая ёмкость дополнительных информационных каналов;
- Синхронная передача и мультиплексирование;
- Высокий уровень стандартизации;
- Надёжная защита трафика.

SDH имеет шесть уровней со скоростями передачи, соответствующими синхронным транспортным модулям STM-N (См. Табл.1). В SDH в качестве среды передачи является оптическое волокно.

Таблица 1 – Уровни иерархии SDH

Уровни иерархии	**Скорость цифрового потока, Мбит/с**
STM – 0	51,84
STM – 1	155,52
STM – 4	622,08
STM – 16	2448,32
STM – 64	9953,28
STM – 256	39813,12

Проектирование сети SDH состоит из следующих этапов [3]:

- Знать следующие исходные данные о сети: количество и расстояния между пунктами связи, количество каналов тональной частоты (КТЧ), количество основных цифровых каналов (ОЦК), количество потока Е1, Е2, Е3 и Е4;
- Рассчитать ёмкость каждого направления;
- Рассчитать ёмкость каждого сетевого тракта;
- Выбрать оптический кабель и выбрать оптический интерфейс на основание типа оптического волокна (См. Рис.1).
- Рассчитать длину регенерационного участка по каждому направлению;
- Рассчитать дисперсию по каждому направлению;
- Рассчитать количество регенерационных участков и количество необслуживаемых регенерационных пунктов (НРП);

Рассчитать оптический бюджет, с целью выяснить устанавливать или не устанавливать оптический усилитель (по причине сильно низкого уровня сигнала на приёме) или аттенюатор (по причине высокого уровня сигнала на приёме).

Расчёт сети SDH при небольшой сети достаточно лёгкий, но, чтобы узнать будет работать сеть по итогам расчёта оптического бюджета можно только в конце всех

расчётов. В случае, если оптический бюджет не удовлетворяет требованиям применяемого оборудования, придётся рассчитывать с самого начала.

Применение / Параметры		Внутри узла	Межузловое соединение						
			Короткая линия		Длинная линия				
Длина волны Источника, нм		1310	1310	1550	1310	1550			
Тип волокна		G.652	G.652	G.652	G.652	G.652,654,655		G.653,655	
Расстояние, км		~2	~15	~15	~40	~80		~80	
Уровень STM-N, Скорость, мБит/С	STM-1 155,52	I-1	S-1.1	S-1.2	L-1.1	L-1.2		L-1.3	
	STM-4 622,08	I-4	S-4.1	S-4.2	L-4.1	L-4.2	U-4.2	L-4.3	U-4.3
	STM-16 2488,32	I-16	S-16.1	S-16.2	L-16.1	L-16.2	U-16.2 V-16.2	L-16.3	U-16.3 V-16.3
	STM-64 9953,28 I-64	S-64.1	S-64.2	L-64.1	L-64.2	V-64.2	L-64.3	U-16.2 V-16.2	U-64.3 V-64.3
	STM-256 39813,12	I-256.2	-	S-256.2	-	L-256.2	-	L-256.3	-

Рисунок 1 – Выбор оптического интерфейса

В случае проектирования больших сетей, например, магистральных требуется произвести огромное количество расчётов, особенно на начальном этапе.

По этой причине, с помощью доступного программного обеспечения MS Excel, было принято решение о создание систему формул, которая оптимизирует и упростит данный расчёт, до уровня ввода исходных данных и ввода параметров, определенных выбранного оборудования.

Рассмотрим работу на примере следующей схемы (См. Рис.2).

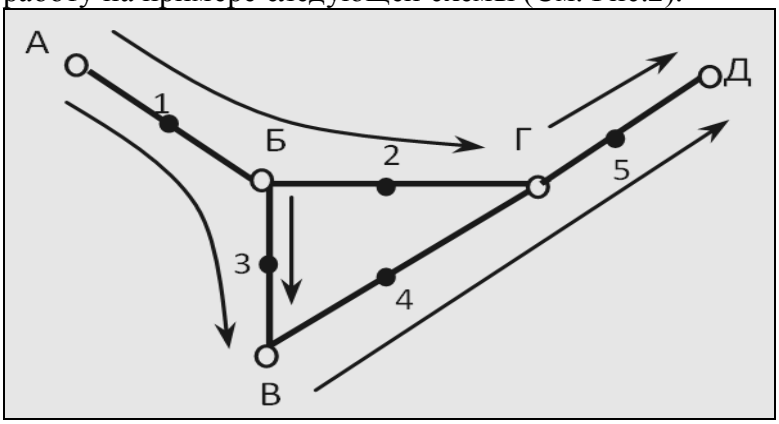


Рисунок 2 – Схема «Треугольник»

На рисунке 2, стрелками указаны направления потоков от пункта к пункту, а каждое соединение между пунктами называется сетевым трактом (пронумерованы от 1 до 5). Исходные данные имеют следующий вид (См. Рис.3).

	A	C	D	E	F	G	H
2	Направление	А-Г	А-В	В-Д	Г-Д	Б-В	
3	Расстояние, км	362	146	136	202	98	
4	Количество КТЧ	123	108	195	0	390	
5	Количество ОЦК	45	54	240	0	288	
6	Количество Е1	5	10	15	20	20	
7	Количество Е2	0	0	0	0	0	
8	Количество Е3	1	1	1	0	0	
9	Количество Е4	0	0	0	0	0	
10							

Рисунок 3 – Исходные данные

Далее необходимо рассчитать количество потоков по каждому направлению, количество потоков E1 считается по следующей формуле в 12 строчке (См. Рис.4):

$$N_{E1} = \frac{N_{\text{КТЧ}}}{30} + \frac{N_{\text{ОЦК}}}{30} + N_{E1}$$

	НАПРАЛЕНИЕ	А-Г	А-В	В-Д	Г-Д	Б-В
12	Всего E1	12	16	30	20	43
13	Всего E2	0	0	0	0	0
14	Всего E3	1	1	1	0	0
15	Всего E4	0	0	0	0	0
16		12 E1+1 E3	16 E1+1 E3	30 E1+1 E3	20 E1	43 E1

Рисунок 4 – Подсчёт потоков по направлениям

Затем необходимо рассчитать количество потоков в каждом сетевом тракте, для это необходимо скопировать готовую формулу из ячейки C25 и растянуть так, чтобы все ячейки были заполнены (См. Рис.5).

	A	C	D	E	F	G	H
18	СЕТЕВОЙ ТРАКТ	СТ 1	СТ 2	СТ 3	СТ 4	СТ 5	
19	Всего E1	121	121	121	121	121	
20	Всего E2	0	0	0	0	0	
21	Всего E3	3	3	3	3	3	
22	Всего E4	0	0	0	0	0	
23		121 E1+3 E3	121 E1+3 E3	121 E1+3 E3	121 E1+3 E3	121 E1+3 E3	
24							
25	А-Г	12	12	12	12	12	
26	А-В	16	16	16	16	16	
27	В-Д	30	30	30	30	30	
28	Г-Д	20	20	20	20	20	
29	Б-В	43	43	43	43	43	
30	А-Г	0	0	0	0	0	
31	А-В	0	0	0	0	0	
32	В-Д	0	0	0	0	0	
33	Г-Д	0	0	0	0	0	
34	Б-В	0	0	0	0	0	
35	А-Г	1	1	1	1	1	
36	А-В	1	1	1	1	1	
37	В-Д	1	1	1	1	1	
38	Г-Д	0	0	0	0	0	
39	Б-В	0	0	0	0	0	
40	А-Г	0	0	0	0	0	
41	А-В	0	0	0	0	0	
42	В-Д	0	0	0	0	0	
43	Г-Д	0	0	0	0	0	
44	Б-В	0	0	0	0	0	
45							

Рисунок 5 – Подсчёт сетевых трактов Этап 1

После того как вокруг заполненных ячеек цифрами будут пустые ячейки (например, ячейка C45 и другие), затем необходимо в диапазоне C25:G29 по каждому сетевому тракту удалить лишние направления, не учитывающие при подсчёте данного сетевого тракта, так как в диапазоне C30:G44 автоматически будут удалены ненужные. Результатом изображен на рисунке 6 (См. Рис.6).

	A	C	D	E	F	G	H
18	СЕТЕВОЙ ТРАКТ	СТ 1	СТ 2	СТ 3	СТ 4	СТ 5	
19	Всего Е1	28	12	59	30	50	
20	Всего Е2	0	0	0	0	0	
21	Всего Е3	2	1	1	1	1	
22	Всего Е4	0	0	0	0	0	
23		28 Е1+2 Е3	12 Е1+1 Е3	59 Е1+1 Е3	30 Е1+1 Е3	50 Е1+1 Е3	
24							
25	А-Г	12	12				
26	А-В	16		16			
27	В-Д				30	30	
28	Г-Д					20	
29	Б-В			43			
30	А-Г	0	0				
31	А-В	0		0			
32	В-Д				0	0	
33	Г-Д					0	
34	Б-В			0			
35	А-Г	1	1				
36	А-В	1		1			
37	В-Д				1	1	
38	Г-Д					0	
39	Б-В			0			
40	А-Г	0	0				
41	А-В	0		0			
42	В-Д				0	0	
43	Г-Д					0	
44	Б-В			0			
45							

Рисунок 6 – Подсчёт сетевых трактов Этап 2

После ввода характеристик интерфейса (ячейки D18 и D19) для каждого, выбора строительной длины кабеля (ячейка C9).

Длина регенерационного участка рассчитывается по следующей формуле:

$$L_{\text{ру}} = \frac{P_s - P_R - P_D - M_{\text{в}} - (N-1)l_{\text{ст}} - N_c l_{\text{стр}}}{a_c + a_m}, \text{км}$$

$$a_m = \frac{l_{\text{ст}}}{l_{\text{стр}}}, \frac{\text{дБ}}{\text{км}}$$

Дисперсия рассчитывается по следующей формуле: $D_{\text{ру}} = D_{\text{км}} * L_{\text{ру}}, \frac{\text{пс}}{\text{нм}*\text{км}}$

Количество регенерационных участков рассчитывается по следующей формуле:

$$n_{\text{ру}} = \frac{L_{\text{тр}}}{L_{\text{ру}}}$$

Количество НРП рассчитывается по следующей формуле:

$$n_{\text{нрп}} = n_{\text{ру}} - 1$$

В ячейке D21 рассчитана длина регенерационного участка, в D24 дисперсия, в D25 количество регенерационных участков, в D26 количество НРП и в ячейке D27 рассчитано оставшееся расстояние от протяженности между пунктами (См. Рис.7).

	A	B	C	D	E	F	G	H	I
7									
8	ПАРАМЕТРЫ СЕТЕВЫХ ТРАКТОВ	S, км		362	146	136	202	98	
9		L (стр)	4	4	4	4	4	4	
10		a (m)	0,02	0,02	0,02	0,02	0,02	0,02	
11		a (c)	0,22	0,22	0,22	0,22	0,22	0,22	
12		l (стр)	0,3	0,3	0,3	0,3	0,3	0,3	
13		N (c)		4	4	4	4	4	
14		l (ст)	0,08	0,08	0,08	0,08	0,08	0,08	
15		N		91	37	34	51	25	
16		M (e)	5	5	5	5	5	5	
17		P (D)	1	1	1	1	1	1	
18		P (R)		-34,5	-34	-34,5	-34	-34,5	
19		P (S)		-3	-5	-3	-5	-3	
20									
21		L (ру)		71	79	90	74	93	
24		D (ру)	18	1278	1422	1620	1332	1674	
25		n (ру)		6	2	2	3	2	
26		n (НРП)		5	1	1	2	1	
27		ОСТАТОК, км		7	67	46	54	5	

Рисунок 7 – Блок ячеек для расчёта регенерационного участка

Далее необходимо рассчитать оптический бюджет, с целью выявить необходимость оптического усилителя или аттенюатора. Тут необходимо ввести вручную максимальную величину уровня сигнала при приёме (ячейка D31) для каждого сетевого тракта.

Уровень передачи сигнала после двух разъемных соединителей рассчитывается по следующей формуле:

$$\mathrm{P_р} = \mathrm{P_{пер}} - 2 * A_р;$$

Далее определяем уровень сигнала после первого неразъёмного соединителя рассчитывается по следующей формуле:

$$\mathrm{P_{н1}} = \mathrm{P_р} - L_{\mathrm{стр}} * \alpha - \mathrm{A_н}$$

Уровень сигнала на выходе i неразъёмного соединителя рассчитывается по следующей формуле:

$$\mathrm{P_{н(i)}} = \mathrm{P_{н(i-1)}} - L_{\mathrm{стр}} * \alpha - \mathrm{A_н}$$

Уровень сигнала на приёме рассчитывается по следующей формуле:

$$\mathrm{P_{пр}} = \mathrm{P_{н(i)}} - 2 * \mathrm{A_н}$$

Рассчитанный уровень приема должен соответствовать условию:

$$\mathrm{P_{пр}}\,min \leq \mathrm{P_{пр}} \leq \mathrm{P_{пр}}\,max$$

В диапазоне ячеек D45:H45 итоговый уровень сигнала после прохождения оптического сигнала в регенерационном участке, а в D47:H47 если стоит «+» значит, уровень сигнала (См. Рис.8).

	A	B	C	D	E	F	G	H	I
28									
29	ПАРАМЕТРЫ РЕГЕНЕРАЦИОННЫХ УЧАСТКОВ	P (пер), дБм		-3	-5	-3	-5	-3	
30		P (пр min), дБм		-34,5	-34	-34,5	-34	-34,5	
31		P (пр max), дБм		-8	-5	-8	-5	-8	
32		Э, дБ	5	5	5	5	5	5	
33		M, дБ	0,05	0,05	0,05	0,05	0,05	0,05	
34		L (с), км		4	4	4	4	4	
35		L (ру), км		71	79	90	74	93	
36		N (р)		4	4	4	4	4	
37		A (р), дБ		0,3	0,3	0,3	0,3	0,3	
38		N (н)		17	19	22	18	23	
39		A (н), дБ		0,08	0,08	0,08	0,08	0,08	
40		α, дБ/км		0,22	0,22	0,22	0,22	0,22	
41									
42	Уровени сигнала от P(р) до P(пр)	P (р), дБм		-3,6	-5,6	-3,6	-5,6	-3,6	
43		n (1), дБм		-4,56	-6,56	-4,56	-6,56	-4,56	
44		n [N (н)], дБм		-19,92	-23,84	-24,72	-22,88	-25,68	
45		P (пр), дБм		-20,52	-24,44	-25,32	-23,48	-26,28	
46									
47		Условие!!!		+	+	+	+	+	

Рисунок 8 – Результаты оптимизации расчёта сети SDH

В результате проделанной работы в ПО «MS Excel» получилось оптимизировать однотипные расчёты для каждого сетевого тракта.

В случае большой проектируемой сети рассчитывать всё вручную долго и можно ошибиться, а с помощью программного обеспечения MS Excel, которое установлено на каждом компьютере можно ускорить расчёты любых сетей SDH.

Направление	А-Г	А-В	В-Д	Г-Д	Б-В					
Расстояние, км	362	146	136	202	98					
Количество КТЧ	123	108	195	0	390					
Количество ОЦК	45	54	240	0	288					
Количество Е1	5	10	15	20	20					
Количество Е2	0	0	0	0	0					
Количество Е3	1	1	1	0	0					
Количество Е4	0	0	0	0	0					

НАПРАЛЕНИЕ	А-Г	А-В	В-Д	Г-Д	Б-В					
Всего Е1	12	16	30	20	43					
Всего Е2	0	0	0	0	0					
Всего Е3	1	1	1	0	0					
Всего Е4	0	0	0	0	0					
	12 Е1+1 Е3	16 Е1+1 Е3	30 Е1+1 Е3	20 Е1	43 Е1					

СЕТЕВОЙ ТРАКТ	СТ 1	СТ 2	СТ 3	СТ 4	СТ 5					
Всего Е1	28	12	59	30	50					
Всего Е2	0	0	0	0	0					
Всего Е3	2	1	1	1	1					
Всего Е4	0	0	0	0	0					
	28 Е1+2 Е3	12 Е1+1 Е3	59 Е1+1 Е3	30 Е1+1 Е3	50 Е1+1 Е3					

А-Г	12	12								
А-В	16		16							
В-Д				30	30					
Г-Д					20					
Б-В			43							
А-Г	0	0								
А-В	0		0							
В-Д				0	0					
Г-Д					0					
Б-В			0							
А-Г	1	1								
А-В	1		1							
В-Д				1	1					
Г-Д					0					
Б-В			0							
А-Г	0	0								
А-В	0		0							
В-Д				0	0					
Г-Д					0					
Б-В			0							

Рисунок 9 – Реализованная работа в ПО «MS Excel»

Конечно, рассмотренный нами метод трудоемок и профессионален (в т.ч. и при использовании универсальных формул в ячейках ПО «MS Excel»). Поэтому для защиты (сохранения) конфиденциальной (персональной) информации необходимы уже более серьезные методы защиты (криптографические и т. п.). Но на уровне пользователя, описанная система обеспечивает нужный уровень безопасности и разграничения доступа.

Перечень использованной литературы и источников:

1. Бирюков Н.Л., Стеклов В.К. Транспортные сети и системы электросвязи. Системы мультиплексирования: Учебник для студентов вузов по специальности «Телекоммуникации» / Под ред. В.К. Стеклова. - К.; 2003, - 352 с.
2. Иванов С.Л., Шамин А.А. Расширение возможностей защиты информации в MS Excel посредством применения макросов / С.Л. Иванов, А.А. Шамин // Вестник НГИЭИ. – 2016. - №4. – С. 94-98. – Серия: Техника и технологии.
3. Литвинович Т.Н. Применение программных комплексов для решения прикладных задач: учеб.-метод. пособие / Т.Н. Литвинович, М.В. Борисенко; М-во трансп. и коммуникаций Республика Беларусь, Белорус. гос. ун-т трансп. – Гомель: бегут, 2018. – 93 с.
4. Общие положения и достоинства SDH. http://biik.ru/uchebnik/csp/page19.html?ysclid=lq53fk7az105967650 (дата обращения: 07.10.2023).
5. Проектирование сетей SDH https://studfile.net/preview/2918838/page:4/(дата обращения: 08.10.2023).
6. Фрейман В.И. Модели, методы и средства диагностирования элементов и устройств распределенных информационно-управляющих систем на основе комбинирования логик: дис. …д-ра тех. наук: 05.13.05 / В.И. Фрейман. – Пермь: Издательство ФГАОУ ВО «ПНИПУ». - 2018. - 418 с.
7. Чернецова Е.А. Системы и сети передачи информации. Часть 1. Телекоммуникационные сети: Монография / Е.А. Чернецова. – СПб.: РГГМУ, 2013. – 244 с.

1.3. СОВРЕМЕННЫЕ МЕТОДЫ И ТЕХНОЛОГИИ ДЛЯ ОРГАНИЗАЦИИ БЕЗОПАСНОЙ РАБОТЫ В СЕТИ ИНТЕРНЕТ

В данной статье рассматриваются современные методы и технологии, которые помогают обеспечить безопасность работы в сети интернет, с учетом разнообразных угроз и вызовов, с которыми сталкиваются пользователи и организации в цифровой эпохе.

Ключевые слова: аутентификация и авторизация, блокчейн-технологии, виртуальные частные сети (VPN), искусственный интеллект (ИИ), кибераналитика, личные данные, машинное обучение, многофакторная аутентификация (MFA), шифрование данных.

MODERN METHODS AND TECHNOLOGIES FOR THE ORGANIZATION OF SAFE WORK ON THE INTERNET

This article discusses modern methods and technologies that help to ensure the security of work on the Internet, taking into account the various threats and challenges faced by users and organizations in the digital age.

Keywords: authentication and authorization, blockchain technologies, virtual private networks (VPN), artificial intelligence (AI), cyber analytics, personal data, machine learning, multi-factor authentication (MFA), data encryption.

С современным увеличением числа пользователей и зависимости от Интернет-сети (Интернет, «всемирная паутина»), обеспечение безопасности при работе в ней стало приоритетной задачей как для частных лиц, так и для организаций. В мире, где множество личных данных, финансовых ресурсов и критической информации переносится и хранится в онлайн-среде, существует неотложная потребность в современных методах и технологиях для обеспечения безопасной работы в сети «всемирной паутины.

Безопасность в Интернет становится все более актуальной темой в наше время, ведь с развитием технологий возрастают и угрозы для персональной и корпоративной безопасности. Множество организаций и частных лиц сталкиваются с рисками связанными с кибератаками, вирусами, фишингом (англ. Phishing от fishing «рыбная ловля, выуживание») – *вид интернет-мошенничества, целью которого является получение доступа к конфиденциальным данным пользователей – логинам и паролям*) и

другими видами мошенничества в сети. Поэтому появляется необходимость в постоянном совершенствовании методов обеспечения безопасности в онлайн-пространстве. Современные методы и технологии играют ключевую роль в этом процессе, обеспечивая защиту как для корпоративных информационных систем, так и для личных данных пользователей.

Рассмотрим несколько способов обеспечения безопасности в Интернет. Использование виртуальных частных сетей (VPN). VPN-сервисы позволяют шифровать интернет-соединение, скрывая данные от посторонних глаз и обеспечивая анонимность в сети. Весь интернет-трафик между ними шифруется, что делает его недоступным для посторонних. VPN позволяет обходить географические ограничения, обеспечивает анонимность и защищает данные при использовании общественных Wi-Fi сетей.

Другим методом обеспечения безопасности является многофакторная аутентификация (MFA). Этот метод требует от пользователя предоставить не только пароль, но и дополнительный фактор, такой как SMS-код, биометрические данные или аппаратное устройство для подтверждения личности, что обеспечивает дополнительный уровень безопасности. Даже если злоумышленник узнает пароль, без второго фактора он не сможет получить доступ.

Антивирусные программы и системы мониторинга обнаруживают и блокируют вредоносные программы, такие как вирусы, трояны и шпионские приложения, обеспечивая защиту от киберугроз. Они также предоставляют защиту от фишинговых атак и вредоносных веб-сайтов.

Не менее важным звеном в обеспечении безопасности являются обновления и патчи (с англ. patch – заплатка, *информация, предназначенная для автоматизированного внесения определённых изменений в компьютерные файлы. Применение патча иногда называется «пропатчиванием»*). Регулярное обновление операционных систем и программного обеспечения предотвращает возможные атаки, включая исправления уязвимостей.

Сетевые брандмауэры контролируют трафик в сети и могут блокировать нежелательные подключения и атаки, защищая от угроз сетевого характера могут фильтровать определенные типы трафика и приложений.

Вместе с тем, облачные решения для безопасной работы в Интернет-сети, обеспечивают удобство использования и надежную защиту данных в облаке. Облачные провайдеры используют шифрование для защиты информации как в покое, так и в движении, и предоставляют механизмы контроля доступа.

Системы на основе искусственного интеллекта (ИИ) и машинного обучения (МО) могут анализировать обширные объемы данных для обнаружения аномалий и угроз. Это позволяет быстро реагировать на потенциальные атаки и минимизировать риски.

Не маловажным аспектом является обучение сотрудников (пользователей) в организациях о правилах безопасности, опасностях фишинга и методах защиты данных является важной частью обеспечения информационной безопасности. Обученные сотрудники (пользователи) вероятнее всего будут избегать многих ошибок, которые могут привести к утечке данных или взлому.

Эти современные методы и технологии объединяются, чтобы обеспечить комплексную безопасность в Интернет-сети, учитывая разнообразные угрозы, с которыми мы сталкиваемся в современном цифровом мире. Они помогают защитить как личные данные, так и корпоративные информационные ресурсы от разнообразных угроз, что особенно важно в наше время, когда киберугрозы становятся все более сложными и распространенными.

На примере нашей страны мы видим, какую роль играет Интернет в сфере информационной безопасности не только обеспечения безопасности внутри страны, но и предотвращение сопутствующих угроз из вне.

В последние годы, активно развиваются и применяются современные кибертехнологии и методы защиты. Повышается проведения экспертиз в области кибербезопасности, и множество IT-компаний (например в России: АО «АЛТЭКС-СОФТ», ЗАО «ДиалогНаука», ЗАО «Защита информации», ООО «Код Безопасности», Центр Безопасности Информации «Маском», ООО НПФ «Радиосервис», ФГУП СКБ ИРЭ РАН, ЗАО «НПО РТК» и т.д.) начали специализироваться на создании инновационных решений для защиты информации и борьбы с киберугрозами. Это включает в себя разработку средств киберзащиты, мониторинг и анализ безопасности корпоративных сетей, а также обучение и консультации сотрудников по кибербезопасности.

Зачастую, киберпреступники в разработке своих программ для проведения атак делают упор прежде всего на детскую и юношескую аудитории населения, ведь дети и молодые люди являются более уязвимыми с психологической точки зрения, поэтому можно легко воздействовать на их мышление с помощью различных средств: несанкционированной рекламы, IT-рекрутинга, блогерские ролики, а также различных приложений для мобильных телефонов, компьютеров и планшетов. В современном мире разработано много средств по предотвращения такого воздействия на детско-юношеские ум и психику, но все равно невозможно полностью исключить факт таких угроз.

Среди современных методов и технологий, которые активно используются IT-сфере мы можем выделить:

- ИИ и МО: современные *IT-компании разрабатывают инновационные алгоритмы для выявления аномалий и предотвращения кибератак.*

- Кибераналитика: *анализ данных и событий в реальном времени помогает выявлять потенциальные угрозы и быстро реагировать на них.*

- Блокчейн-технологии: *помогают активно разрабатывать решения, использующие блокчейн для обеспечения целостности данных и защиты от мошенничества.*

- Обучение пользователей: *важной частью обеспечения информационной безопасности является обучение сотрудников и граждан правилам кибербезопасности, проведение информационных кампаний и образовательных мероприятий.*

В нашей стране налаживаются связи и сотрудничество с другими странами и международными организациями по вопросам кибербезопасности. Мы становимся участниками в мероприятиях по борьбе с киберугрозами. Современные технологии и методы в области кибербезопасности применяются, как для защиты государственных интересов, так и для обеспечения безопасности частных лиц и компаний в цифровой среде.

Еще одна сторона работы с сетью является борьба с дезинформацией.

Дезинформация в Интернет-сети представляет собой распространение ложной или вводящей в заблуждение информации с целью воздействия на общественное мнение, создания хаоса или достижения политических целей. Современная политическая ситуация в мире нестабильна, каждая сфера нашей жизни охвачена и зависит от этого положения. Важно рассматривать все аспекты нашего времени, мы живем в век, быстро развивающихся информационных технологий, не стоит исключать факт ведения информационно-психологической войны. Киберпреступники создают дезинформацию и распространяют ее среди населения, такие действия могут привести к пагубным последствиям. Однако, каждый человек сам может выбирать какую информацию воспринимать, но некоторые люди не в состоянии отличить ложь от правды, поэтому важно обеспечивать безопасную работу в Интернет-сети.

Для противодействия дезинформации используют: мониторинг, факт-чекинг (*процесс проверки фактической точности сомнительных сообщений и заявлений.*

Проверка фактов может осуществляться до (ante hoc) или после (post hoc) публикации или иного распространения текста или контента), блокчейн-технологии (*усовершенствованный механизм базы данных, который позволяет организовать открытый обмен информацией в рамках бизнес-сети*).

- Мониторинг социальных медиа: *многие дезинформационные кампании начинаются в социальных медиа. Современные инструменты могут помочь выявить аккаунты и группы, распространяющие дезинформацию.*

- Факт-чекинг: *существуют специализированные IT-организации и инструменты для проверки фактов и опровержения ложной информации. Автоматизированные системы могут помочь идентифицировать фейковые новости.*

- ИИ и МО: *данные технологии могут помочь в анализе больших объемов данных, выявлении паттернов (*от англ. pattern – «узор, образец, шаблон; форма, модель; схема, диаграмма»: схема-образ, действующая как посредствующее представление, или чувственное понятие, благодаря которому в режиме одновременности восприятия и мышления выявляются закономерности, как они существуют в природе и обществе*) и аномалий в распространении дезинформации.*

- Блокчейн-технологии: *блокчейн может использоваться для создания системы подтверждения достоверности информации. Это может помочь предотвратить подделку данных и документов.*

Образование и обучение: *обучение пользователей и общества основам критического мышления и различению надежных и ненадежных источников информации играет ключевую роль в борьбе с дезинформацией.*

Современные методы и технологии в области кибербезопасности и анализа данных помогают обнаруживать, анализировать и предотвращать дезинформацию, это становится актуальным в цифровом мире, где распространение ложной информации имеет серьезные последствия для общества и политики.

Рассмотрим конкретные примеры современных методов и технологий в борьбе с дезинформацией в Интернет-сети. К ним принято относить:

- *Факт-чекинг-организации:* IT-организации, такие как «Snopes», «FactCheck.org» и «PolitiFact», проводят независимую проверку фактов и опровергают ложную информацию в новостях и социальных медиа. Они используют ресурсы и экспертов для подтверждения или опровержения утверждений, предоставляя публике достоверную информацию.

- *Инструменты для анализа социальных медиа:* существуют программные инструменты и аналитические платформы, такие как «CrowdTangle» и «Hoaxy», которые помогают отслеживать и анализировать распространение информации в социальных медиа. Они могут выявить вирусные тренды и аккаунты, активно распространяющие дезинформацию.

- *Машинное обучение для обнаружения фейковых новостей:* ИИ и МО используются для создания алгоритмов, способных выявлять фейковые новости и дезинформацию на основе паттернов и характеристик таких материалов.

- *Блокчейн для подтверждения достоверности информации:* некоторые стартапы и проекты разрабатывают системы блокчейна, которые позволяют подтверждать достоверность и происхождение информации. Это может быть полезно для новостных организаций и сайтов.

- *Сотрудничество между платформами и государствами:* популярные социальные медиа-платформы, такие как «ВКонтакте» и «Telegram», сотрудничают с правительствами и организациями по борьбе с дезинформацией. Они могут блокировать или удалять ложную информацию и аккаунты.

- *Образовательные программы и кампании:* различные образовательные организации и правительственные агентства проводят семинары по повышению осведомленности об опасностях дезинформации и обучению критическому мышлению.

В современном мире, с развитием информационных технологий, увеличивается количество фейков и поддельных страниц в сети, представляющих потенциальную угрозу для правильного восприятия ситуации и возможности мошенничества в онлайн-пространстве [1, с 93]. Эта проблема не ограничивается только государственной информацией, она затрагивает интересы обычных граждан.

Важно отметить, что низкий уровень правовой грамотности населения усугубляет ситуацию. Неправильное использование интернет-ресурсов приводит к недопониманию доступной информации, что означает, что родители не всегда могут обеспечить безопасность своих детей в онлайн-пространстве. Подростки становятся жертвами незаконных сайтов, взрослые подвергаются воздействию фейковых новостей. Такие *«войны и миры»* легко влияют на общественное мнение, при этом подлинность информации часто остается непроверенной.

Обратимся к данным, проливающим свет на динамику фейков в период с 2021 по 2024 год. В таблице 1 представлены количественные показатели фейков для каждого из этих лет, отражая нарастающую тенденцию или, возможно, успешные усилия по их сдерживанию.

Таблица 1 – Количество Фейков за 2021-2024 года

Количество фейков	**2021 год**	**2022 год**	**2023 год**	**2024 год**
	1,5 млн.	9 млн.	12,5 млн.	~22 млн.

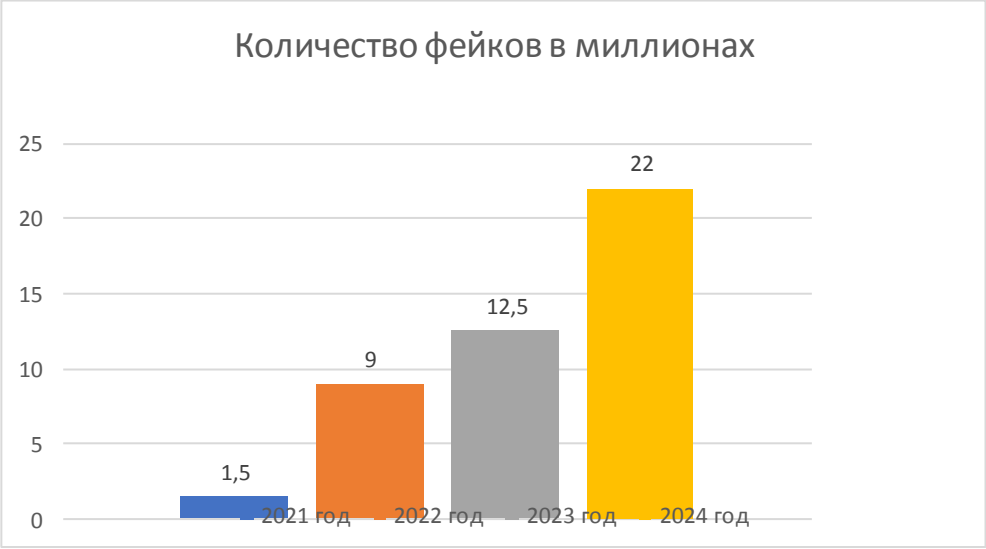


Рисунок 1 – График количества фейков в миллионах

Эти цифры не только отражают масштаб проблемы, но и служат метрикой для оценки эффективности принимаемых мер по борьбе с фейками. Решение этой проблемы требует не только технических инноваций, но и образования общества, поддержки родителей и разработки сбалансированных стратегий информационной безопасности. С каждым годом показатели увеличиваются, это связано с тем, что появляется все больше и больше новых технических средств и методов связи, именно поэтому важно своевременно устранять информационные фейки [2, с 545].

Правила обеспечения информационной безопасности всем известны, это создание персональных паролей, использование проверенных браузеров, сайтов. Не рекомендуется размещать в свободном доступе информацию о себе и своих близких. Об этом говорят постоянно по телеканалам, предупреждают в общественном транспорте. Почему же тогда такие преступления все равно имеют место. Самое распространенное это мошенничество с помощью телефонных звонков. Следует отдать должное мошенники, которые звонят по телефону, очень хорошо осведомлены, о человеке, которому они звонят, это раз, во-вторых, они хорошие психологи, знают, как

разговорить человека, особенно если этот человек пожилого возраста. Поэтому следует ознакомить с правилами безопасности своих родственников и знакомых, которые в силу возраста или недостаточного уровня финансовой грамотности могут быть особенно уязвимы для действий киберпреступников.

Лавинное распространение получили угрозы «Нулевой день» – это общий термин, он описывает недавно обнаруженные уязвимости в системе безопасности, которые могут быть использованы злоумышленниками для атаки на систему. В этом случае поставщик или разработчик только что узнали об уязвимости, и у них есть «ноль дней» на ее исправление. Происходит это, потому что развитие информационной области идет с большой скоростью, а люди естественно подстраиваются под это. И как мы видим из диаграммы, динамика инцидентов в области информационной безопасности растет (См. Рис. 2) [3, с 24].

Анализируя причины распространения нарушений, в сфере информационных технологий мы приходим к выводу, по статистике в России раскрывается меньше 25% киберпреступлений. Чувствуя безнаказанность, преступники с каждым годом совершенствуют методы кибернетических атак. Следует отметить, что наибольшее количество преступлений совершается с использованием электронных средств платежей и в сфере компьютерной информации. Это происходит, потому что для создания вредоносной программы нужно время и знания, как и для доступа к информации.

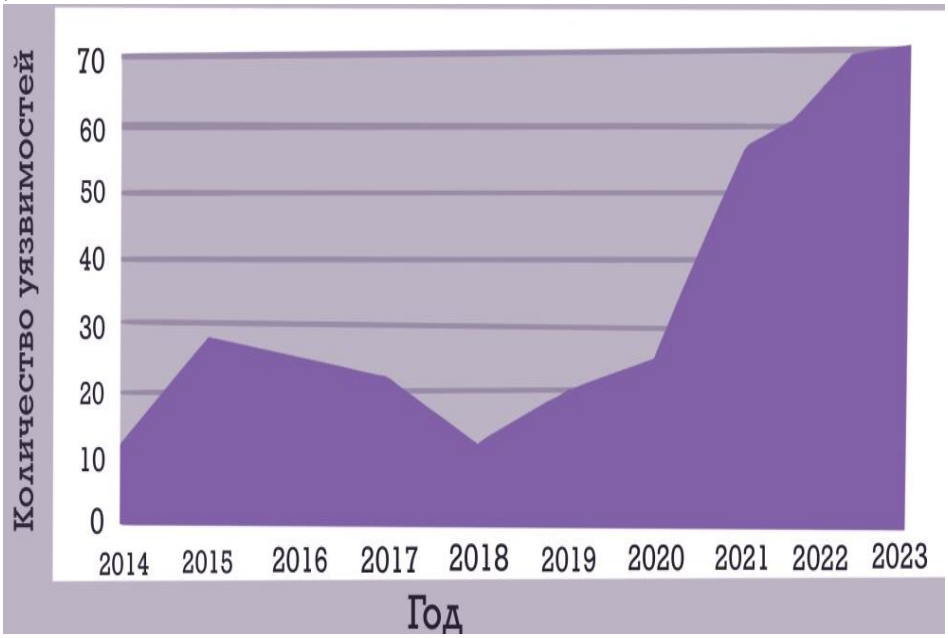


Рисунок 2 – Количество угроз нулевого дня

В заключение, ограничение доступа к сети не ведёт к решению проблемы, наоборот, усугубляет ситуацию. В современном цифровом мире безопасность в сети интернет становится важной задачей, требующей комплексного подхода и использования современных технологий. Виртуальные частные сети (VPN) обеспечивают шифрование данных, многофакторная аутентификация (MFA) повышает уровень защиты аккаунтов, а браузеры с усиленной безопасностью предоставляют дополнительные функции защиты при интернет-серфинге. Важно отметить, что решение проблемы фейков требует не только технических инноваций, но и образования общества. Осведомленность об угрозах и разработка сбалансированных стратегий информационной безопасности являются неотъемлемой частью этого процесса.

Правила безопасности в сети, такие как создание надежных паролей, использование проверенных браузеров и сайтов, а также ограничения размещения

личной информации в открытом доступе, остаются актуальными и важными для предотвращения киберпреступлений.

Перечень используемой литературы и источников:

1. Зобова Е.В., Котова А.Е., Коваленко Т.А. Алгоритм нахождение фейков // Всероссийская научно-практическая конференция «Профессиональные и технологические аспекты разработки отечественного программного обеспечения», посвященная 30-летию кафедры программного обеспечения вычислительной техники и автоматизированных систем. сб. науч. тр. (Оренбург, 13-14 сентября 2023 года). – Оренбург: Изд-во ОГУ, 2023. – С. 92-99.
2. Котова А.Е., Зобова Е.В., Коваленко Т.А. Путь к правде: как распознать и бороться с фейковыми новостями // Инновационные инфокоммуникации XXI века: 24-я (XXIV) Всероссийская студенческая научная (очно-заочная) конференция, посвященная Дню Радио, 78-й годовщине Победы советского народа над фашисткой Германией в Великой Отечественной войне 1941-1945 гг. и Десятилетию науки и технологий в Российской Федерации (Хабаровск, 27 апреля - 5 мая 2023 года). [Электронное научное издание 1 – Файл: 17,2Мб]. – URL: https://hiik.ru/about_the_university/nauka-i-innovatsii / Председатель редакционной коллегии, профессор, д.т.н. С.И. Смагин и др. – Хабаровск: Изд-во ХИИК СибГУТИ, 2023. – С. 545-548.
3. Коваленко Т.А., Леутина А.Н. Правонарушения в сфере информационных технологий /Т .А. Коваленко, А.Н. Леутина // Наука и бизнес: Пути развития. – 2023. - №10 (148). – С. 21-24.
4. Киберпреступность в мире. [Электронный ресурс]. – URL: https://www.tadviser.ru/index.php (Дата обращения: 18.10.2023).

1.4. ИСКУССТВЕННЫЙ ИНТЕЛЛЕКТ В СОВРЕМЕННОМ МИРЕ

Человек, высшее животное – это сложные высокоорганизованные биологические системы, обладающие когнитивными способностями. Если искусственная система, например, робот, также может их демонстрировать, то эту систему можно отнести к искусственным интеллектуальным системам. «Еще недавно предполагалось, что искусственный интеллект – это заложенное в памяти программы решение, т.е. не новое решение (творческая функция), а алгоритм, содержащий решение в вычислительной программе... В начале развития робототехники предполагалось, что робот выполняет действия только по ранее заданным программой алгоритмам. Искусственный интеллект – это следующая стадия развития робототехники и программирования (их особая часть), наделяющая способностью робота самостоятельно принимать «новое» решение, ранее не заложенное в программе» [1]. Сегодня искусственным интеллектом (ИИ) признается полностью или частично автономная самоорганизующаяся система, обладающая возможностями мыслить, обучаться, самостоятельно принимать решения.

Ключевые слова: интеллект, интеллектуальный агент (ИА), интернет-пользователь, искусственный интеллект (ИИ), ИТ-компании, сеть Интернет, цифровые технологии (ЦТ).

ARTIFICIAL INTELLIGENCE IN THE MODERN WORLD

Man, the higher animal, are complex highly organized biological systems with cognitive abilities. If an artificial system, for example, a robot, can also demonstrate them, then this system can be attributed to artificial intelligent systems. "Until recently, it was assumed that artificial intelligence is a solution embedded in the program's memory, i.e., not a new solution (a creative function), but an algorithm containing a solution in a computational program... At the beginning of the development of robotics, it was assumed that the robot performs actions only according to algorithms previously set by the program. Artificial intelligence is the next stage in the development of robotics and programming (their special part), which gives the robot the ability to independently make a "new" decision that was not previously included in the program" [1]. Today, artificial intelligence (AI) is recognized as a fully or partially autonomous self-organizing system with the ability to think, learn, and independently accept.

Keywords: intelligence, intelligent agent (IA), Internet user, artificial intelligence (AI), IT-companies, the Internet, digital technologies (CT).

Под интеллектом обычно понимается свойство психики человека, позволяющее ему правильно интерпретировать получаемые извне данные и адаптироваться к новым ситуациям. Человек обладает когнитивными способностями или когнитивными

функциями – это высшие функции мозга, они связывают человека с окружающим миром, позволяя получать представление о нем и взаимодействовать с ним. К когнитивным способностям можно отнести мышление, речь, обучаемость, ориентирование в пространстве и т.д. Интеллект – проявление когнитивных способностей. Интеллект определяется многими способами: способности более высокого уровня (такие как абстрактное мышление, мысленное представление, решение проблем и принятие решений), способность к обучению, эмоциональные знания, творчество и адаптация для эффективного удовлетворения требований окружающей среды.

Искусственный интеллект (ИИ) – это способность искусственных интеллектуальных систем проявлять когнитивные функции: обучаться, в том числе на собственном опыте, подстраиваться под заданные параметры и выполнять задачи, которые ранее были доступны только человеку (или высшим животным).

ИИ, вероятно, является определяющей технологией последнего десятилетия, и, возможно, также следующий. Искусственный интеллект настолько интегрировал в повседневную жизнь, что человек едва ли взаимодействует с какой-либо технологией, не сталкиваясь с ней. Эта интеграция ИИ также проникла в правоохранительную деятельность, позволив сотрудникам более эффективно раскрывать различные преступления, а также постоянно развивающиеся киберпреступления.

Первоначально введенный в 1955 году американским специалистом в области информатики, доктором математики Джоном Маккарти (1924-2011), термин «искусственный интеллект» [2] определялся как: «наука и техника создания интеллектуальных машин» [3]. Несмотря на многочисленные преимущества программного обеспечения на основе ИИ, многие все еще обеспокоены легитимностью этих систем. Тем не менее, многие IT-компании признают преимущества, которые может принести это новое партнерство между компьютерами и людьми, и постоянно исследуют и разрабатывают инновационные способы использования этой технологии. Сегодняшние определения ИИ часто включают другие требования, такие как автономия, и позволяют ограничить данное определение определенными областями наук.

ИИ относится к системам, которые демонстрируют интеллектуальное поведение, анализируя окружающую среду и предпринимать различные действия, с некоторой степенью автономии, для достижения конкретных целей. Ранее сказанное нами не накладывает ограничений на методы, используемые для достижения определенного интеллекта.

ИИ – это общий термин, включающий в себя широкий спектр технологий и приложений, которые имеют немного больше возможностей.

Термин «искусственный интеллект» регулярно используется для обозначения любой техники, используемой в любом контексте – реальном или воображаемом. Интеллект отображает функции, которые некоторые называют интеллектуальными.

Программа ИИ называется – «интеллектуальным агентом» (ИА). Программа ИА получает возможность взаимодействовать с окружающей средой. ИА может определять состояние среды с помощью своих датчиков, а затем влиять на состояние с помощью своих исполнительных механизмов. Важным аспектом ИИ является политика ИА, которая подразумевает, как входные данные, полученные от датчиков, передаются

исполнительным механизмам, другими словами, то, как датчики сопоставляются с исполнительными механизмами, становится возможным благодаря функции внутри агента.

Конечной целью ИИ является развитие человеческого интеллекта в машинах. Однако такую мечту можно осуществить с помощью алгоритмов обучения, которые пытаются имитировать процесс обучения человеческого мозга. ИИ медленно, но, верно, становится действенным инструментом наказания преступника, а также пресечения противоправных действий. Многие правоохранительные органы по всему миру используют самые современные решения для предотвращения преступлений. Одним из таких решений является «распознавание лиц», которое широко применяется в различных областях, помимо права, для обеспечения безопасности.

ИИ революционизирует отрасли благодаря своим приложениям и помогает решать сложные проблемы. ИИ можно использовать практически во всех сферах деятельности, получая новые возможности для людей. Применение ИИ может осуществляться с целью освобождения человека от монотонной работы, для автоматизации опасных видов работ, поддержки в принятии решений и поддержания коммуникаций между людьми.

Цифровые технологии (ЦТ) – это технологии, обеспечивающие цифровую трансформацию экономики и общества в целом, они основаны на сохранении и передаче информации в преобразованном в цифры формате.

Технологии ИИ – это группа ЦТ, делающих возможным выполнение задач, для осуществления которых ранее требовалось использование когнитивных способностей человека (распознавание речи и визуальных образов, принятие аналитических решений, сложные логические операции, предсказание будущего на основе накопленных данных и т.д.). Данная группа технологий тесно взаимодействует с другими группами ЦТ - именуемых «сквозными» [4,5].

Размышление об ИИ может показаться размышлением о фантастическом мире, похожем на мир из научно-фантастических фильмов, но на самом деле границы между реальностью и вымыслом стираются. Искусственный интеллект меняет мир и жизнь людей и становится двигателем роста экономик и организаций. Будь то простой поиск в «Google», разговор с «Google Home» или «Siri» от «Apple», или простой чат-бот на каком-то веб-сайте, который вы посетили. Это, без сомнения, меняет то, как мы выполняем нашу повседневную деятельность, организуем нашу работу и то, как мы принимаем решения в нашей повседневной жизни.

Развитие «сквозных» технологий, их внедрение в производство и сферу услуг стимулируется практически всеми государствами, так как позволяет повысить уровень технологического развития страны и конкурентоспособность национальной экономики по отношению к другим странам. Подобные технологии обеспечивают основы цифровой трансформации общества, интегрируя во все аспекты деятельности и требуя масштабных изменений производственной культуры, меняя сами принципы создания продуктов и предоставления услуг.

ИИ уже давно используется в различных секторах, таких как транспорт, финансы, энергетика, здравоохранение и т.д. По сравнению с этими секторами, полиция совсем недавно приняла ИИ. Многие страны по всему миру узнали о его преимуществах и потенциале против преступников, а также в раскрытии преступлений. Хотя ИИ в полиции все еще находится на прогрессивной стадии, но результаты того стоят. Он имеет склонность бороться практически со всеми видами преступлений, для которых он считается влиятельным инструментом. Это дает правоохранительным органам возможность сосредоточить свои активы в определенном месте и в определенное время. Прежде чем проводить какую-либо операцию в районе, очень важно знать этот участок земли. Такую важную информацию можно получить с помощью дронов, оснащенных датчиками.

Использование ИИ способно повысить благосостояние общества и качество жизни людей. По преобразующему воздействию на общество искусственный интеллект сравнивают с электричеством, которое в свое время полностью изменило производство, выведя экономику на принципиально новый уровень развития, и поменяло технологический уклад в мире. Внедрение ИИ в промышленность ускоряет цифровизацию экономики, стимулируя развитие информационной-телекоммуникационной инфраструктуры на территории страны и повышает долю отечественного программного обеспечения на внутреннем и внешнем рынках.

Технологиями ИИ в широком плане это: «…программное обеспечение, способное выполнять задачи, для выполнения которых традиционно требуется использование когнитивных способностей человека – распознавание речи и визуальных образов, принятие аналитических решений, сложные логические операции, предсказание будущего на основе накопленных данных и т.п.» [5,6].

Основной технологий ИИ является способность компьютерных систем к «самообучению», использованию накопленных данных или специально созданной среды для программирования определенных правил принятия решений или поведения, применимых в будущем. Главным идеологическим отличием технологий ИИ от традиционных цифровых решений является тот факт, что при выполнении задач они не опираются на логические схемы, заданные программистами, а сами выстраивают комплексные механизмы принятия решений («нейронные сети») на основе тех данных и задач, что были поставлены программистами.

Следует отметить, что различные варианты технологий ИИ не являются будущими возможностями, а являются сегодняшними реалиями, которые разрабатываются и проверяются академическими и научными исследователями, а в некоторых случаях правоохранительными органами и службами безопасности [1].

Эффективная работа с ИИ во многом зависит от доверия общества. Общественная безопасность может быть поставлена под угрозу, когда население теряет доверие.

ИИ медленно, но, верно, становится действенным инструментом наказания преступника, а также пресечения противоправных действий. Многие правоохранительные органы по всему миру используют самые современные решения для предотвращения преступлений. Одним из таких решений является «распознавание лиц», которое широко применяется в различных областях, помимо права, для обеспечения безопасности.

ИИ уже давно используется в различных секторах, таких как транспорт, финансы, энергетика, здравоохранение и т.д. Поскольку это относительно новая технология, люди часто не до конца понимают, как на самом деле работает искусственный интеллект и что он может, а что нет. Это позволяет размножаться беспокойству и страху, и при неправильных обстоятельствах эти чувства могут помешать интеграции и применению технологии. Возможно, нигде это не является более важным, чем когда речь идет об использовании искусственного интеллекта в государственном секторе и, в частности, в правоохранительных органах. Например, полиция использует камеры ИИ для помощи при осмотре мест преступления. Иногда место преступления распространяется на большую территорию, которая становится недоступной для пеших прогулок. ИИ в полиции поможет обеспечить понимание в такой ситуации. Это может даже помочь в поиске улик после совершения преступления. Помимо камеры, правоохранительные органы также полагаются на видеотехнологии, чтобы внимательно следить за сомнительными угрозами всякий раз, когда собирается большое скопление людей. В основном во время фестивалей и крупных спортивных мероприятий ИИ используется для обнаружения любых неблагоприятных инцидентов. Использование видеотехнологий также позволяет осуществлять наблюдение посредством распознавания лиц, поскольку оно помогает

идентифицировать лица людей в огромной толпе.

Перечень используемой литературы и источников:
1. Лаптев В.А. Понятие искусственного интеллекта и юридическая ответственность за его работу / В.А. Лаптев // Право. Журнал Высшей школы экономики. – 2019. - № 2. – С. 83.
2. Маккарти Джон // Большая советская энциклопедия: [в 30 т.] / под ред. гл. ред. А. М. Прохоров. – 3-е изд. – Москва: Советская энциклопедия, 1969.
3. Морхат П.М. К вопросу об определении понятия искусственного интеллекта / М.П. Морхат // Право и государство: теория и практика. – 2017. - № 12(156). – С. 25-32.
4. Рассел С., Норвиг П. Искусственный интеллект: современный подход / С. Рассел, П. Норвиг; [пер. с англ. и ред. К. А. Птицына]. - 2-е изд. - Москва: ИД «Вильямс», 2006. - 1407 с.
5. Эндрю А. Искусственный интеллект / А. Эндрю, пер. с англ. пер. В.Л. Стефанюк; под ред. и с предисл. Д.А. Поспелова. – Москва: Мир, 1985. – 264 с.
6. Яцуренко А. Абсолютный алгоритм. Проблемы развития искусственного интеллекта / А. Яцуренко [Электронный ресурс] // Новый оборонный заказ. Стратегии. – 2021. - № 5 (70). – URL: https://dfnc.ru/arhiv-zhurnalov/2021-5-70/absolyutnyj-algoritm-problemy-razvitiya-iskusstvennogo-intellekta/ (дата обращения: 20.12.2023).

1.5. СПОСОБЫ ОЦЕНКИ ЭФФЕКТИВНОСТИ ИНФОРМАЦИОННОГО ОБМЕНА В ЦИФРОВЫХ СИСТЕМАХ СВЯЗИ С УЧЕТОМ ИНФОРМАЦИОННЫХ ПОТЕРЬ

На основе анализа общеизвестных подходов к оцениванию информационной эффективности цифровых систем связи обоснована актуальность осуществления оценки с учетом допустимых информационных потерь в условиях изменения интенсивности входного трафика и воздействия дестабилизирующих факторов. Выбран обобщенный показатель оценки – удельная интегральная нагрузка системы, характеризующая ее возможности по передаче и хранению информации. Разработаны способы текущей и интервальной оценки эффективности информационного обмена в цифровой системе связи с учетом обеспечения допустимых информационных потерь. Показаны возможности практической реализации полученных способов на основе существующей элементной базы и сформулированы рекомендации по их использованию для адаптации цифровых систем связи к изменениям входного трафика и воздействию дестабилизирующих факторов.

Ключевые слова: входной трафик, дестабилизирующие факторы, информационные потери, обобщенный показатель, оценка эффективности, цифровая система связи.

WAYS TO ASSESS THE EFFECTIVENESS OF INFORMATION EXCHANGE IN DIGITAL COMMUNICATION SYSTEMS TAKEN INTO ACCOUNT OF INFORMATION LOSSES

Based on an analysis of well-known approaches to assessing the information efficiency of digital communication systems, the relevance of the assessment is substantiated, taking into account acceptable information losses in conditions of changes in the intensity of input traffic and the impact of destabilizing factors. A generalized evaluation indicator has been selected - the specific integral load of the system, which characterizes its capabilities for transmitting and storing information. Methods have been developed for current and interval assessment of the effectiveness of information exchange in a digital communication system, taking into account the provision of acceptable information losses. The possibilities of practical implementation of the obtained methods based on the existing element base are shown and recommendations are formulated for their use for adapting digital communication systems to changes in input traffic and the effects of destabilizing factors.

Keywords: input traffic, destabilizing factors, information losses, generalized indicator, efficiency assessment, digital communication system.

Введение. Анализ функционирования цифровых систем связи (ЦСС) в условиях резких изменений входного трафика ($\gamma_{вх}$) и воздействия дестабилизирующих факторов показывает, что при определенном значении интенсивности информационной нагрузки в ЦСС возникают существенные потери информационных пакетов

(информационные потери), которые необходимо учитывать и по возможности минимизировать. Для решения этой задачи требуется проведение адекватной оценки эффективности информационного обмена (информационной эффективности) ЦСС, обеспечивающей правильный учет доли потерянных пакетов в значении обобщенного показателя и выбор наилучших условий функционирования системы с минимальными потерями информации [1]. При этом требуется не только точечная (при текущем значении входного трафика), но и интервальная оценка информационной эффективности ЦСС, позволяющая определить область качественной работы системы на основе определения возможностей по передаче и хранению информации, исходя из заданных технических требований и ограничений. Таким образом, актуальной является задача разработки способов оценки эффективности информационного обмена в ЦСС с учетом допустимых информационных потерь на основе обобщенного показателя. Применение такого подхода, в свою очередь, может быть использовано для рационального распределения системных ресурсов в реальном масштабе времени (адаптации ЦСС к условиям функционирования) и обоснования научно-практических рекомендаций, определяющих выбор наиболее благоприятных условий использования ЦСС при различных значениях интенсивности входного трафика и воздействии дестабилизирующих факторов.

Анализ известных подходов к оценке информационной эффективности ЦСС. Формулирование цели исследования. Обзор рассматриваемой в работе предметной области исследований показывает, что известны многие способы, параметры и показатели оценки эффективности информационного обмена в ЦСС, которые, в целом, условно можно объединить в три общие, по основным признакам, группы [1 – 6].

К первой группе относятся локальные параметры информационной эффективности ЦСС. Так для оценки качества передачи информации по каналам связи (КС) ЦСС (на канальном уровне) используются: пропускная способность или максимальная скорость передачи информации по КС – C (для дискретного КС с ошибками определяется известной формулой Шеннона); текущая и средняя за заданный интервал времени скорость передачи в КС – R; коэффициент использования канала $\mu = R / C$, отражающий долю пропускной способности КС, которая используется для осуществления для информационного обмена [1 – 3]. При этом свойство временного хранения информации в ЦСС оценивается показателями: средняя временная задержка одного пакета в системе T и количество пакетов N, находящихся на хранении в буферных запоминающих устройствах узлов коммутации (УК). Для оценивания эффективности информационного обмена на сетевом уровне используются следующие параметры: производительность системы $G = N_{уп} / \Delta T$, как количество успешно переданных пакетов $N_{уп}$ за заданный интервал времени наблюдения ΔT; количество потерянных пакетов $N_{пот}$. Отдельно для учета воздействия дестабилизирующих факторов в итоговой оценке учитываются значения показателей помехоустойчивости: вероятности битовой ошибки $P_{ош}$ (BER) или ее логарифма S, вероятности потери пакета $P_{пот}$ [4]. Кроме того, к первой группе относятся QoS-параметры (Quality of Service), которые получили широкое применение в практических приложениях. В этом случае дополнительно учитываются колебания временной задержки – джиттер ΔT_d [1]. Для оценки своевременности и достоверности доведения информации до получателя используются вероятностно-временные характеристики:

функция распределения времени доведения $F_{T_д}(t)$ и вероятность своевременной доставки пакетов $P_{св}(t)$, а также функция достоверности D [1, 3, 6].

Вторая группа содержит информационно-технические показатели эффективности, которые дополнительно оценивают живучесть системы, достоверность доведения информации и качество выбранных технических решений при построении отдельных элементов и ЦСС в целом [4]. За основной показатель при этом принят коэффициент достоверности

$$\gamma_{ИТ} = lg\left(\frac{P_{ош}}{P_{ошd}\left(\frac{T_{kkd}}{T_{kk}} + \beta_э \frac{N_{эad}}{N_{эа}}\right)}\right), \quad (1)$$

где $P_{ош}$, T_{kk} – соответственно вероятность битовой ошибки BER и средняя длительность кодовой комбинации до применения способа повышения достоверности; $P_{ошd}$, T_{kkd} – те же величины после применения способа повышения достоверности; $N_{эad}$, $N_{эа}$ – число элементов аппаратуры с устройством повышения достоверности и без него, соответственно; $\beta_э$ – весовой коэффициент, обеспечивающий положительное значение $\gamma_{ИТ}$.

В третью группу технико-экономических показателей сведены многокритериальные и векторные характеристики, оценивающие совместно с информационными и техническими, также экономические (эксплуатационные) аспекты реализации и функционирования ЦСС. При этом основные показатели данной группы базируются на принципах обеспечения минимума затрат ресурсов и максимума достигаемого эффекта

$$З_{min} = \min_{x \in X} З(x), \text{ при } Э(x) \in Э^*; \quad (2)$$

$$Э_{max} = \max_{x \in X} Э(x), \text{ при } З(x) \in З^*, \quad (3)$$

где $З(x)$ и $Э(x)$ – функции затрат и достигаемого эффекта; X – множество допустимых вариантов организации системы; $Э^*$ и $З^*$ – допустимые области изменения эффекта и затрат, соответственно.

К ним можно отнести: вектор эффективности функционирования ЦСС $Y_Ф$, включающий оценки систем информационного обмена и управления; многокритериальный матричный показатель, состоящий из векторов-столбцов качественных $Э_к(t)$, системных $Э_с(t)$ и эксплуатационных характеристик $Э_э(t)$ системы [6]; обобщенный технико-экономический показатель $\gamma_{ТЭ}$, оценивающий экономические затраты при создании, разработке и эксплуатации ЦСС в течение времени существования системы; показатели суммарного риска $R_{СИС}$ системы (через значения текущего риска КС $R_{тек}$), которые, в конечном счете, определяют показатели средних $R_{СМП}$ и общих $R_{ОМП}$ материальных потерь пользователя [4]; наконец обобщенный параметр, который характеризует удельную себестоимость ЦСС с учетом производительности и достоверности передачи информации (выражается в единицах: руб./(пакет/с)3)

$$Ливн = S /(GR_{дост} T_{ПИ}), \quad (4)$$

где S – затраты на организацию и эксплуатацию ЦСС; $R_{дост}$ – скорость доставки пакетов, $T_{ПИ}$ – точность передачи информации [5].

Анализ рассмотренных групп общеизвестных показателей оценки информационной эффективности ЦСС позволил выявить ряд их общих серьезных недостатков, дополнительно усиливающих значимость данной работы. К их числу можно отнести следующие: в итоговых оценках присутствуют только скоростные характеристики информационного обмена (и только косвенно рассматриваются возможности промежуточного хранения информации); в процессе оценивания не учитывается сетевая структура (производится разбиение топологии на совокупность одноканальных систем (ОС)); получаемые параметры не могут обеспечить адекватное сравнение различных ЦСС при осуществлении информационного обмена и не позволяют оценить их потенциальные возможности по передаче и хранению информации, в том числе учесть влияние потерь информационных пакетов на значение итоговой оценки. Вследствие вышесказанного, данные подходы не могут обеспечить формирование обоснованных научно-практических рекомендаций для организации функционирования ЦСС в зависимости от изменения условий информационного обмена.

Цель данной работы состоит в расширении функциональных возможностей и повышении достоверности оценочного аппарата ЦСС путем разработки способов оценки эффективности информационного обмена с учетом информационных потерь.

Способ текущей оценки эффективности информационного обмена в ЦСС с учетом информационных потерь. Первым шагом на пути реализации поставленной цели исследования был выбор обобщенного показателя оценки информационной эффективности ЦСС в условиях изменения интенсивности входного трафика $\gamma_{вх}$. В работе [7] на основе аналогий с классическим моделями Л. Клейнрока был обоснован и предложен обобщенный показатель – удельная интегральная нагрузка (УИН) ЦСС

$$P = NG|_{T \le T_{доп}}, \qquad (5)$$

где N – среднее количество пакетов, находящихся в системе на хранении; G – средняя производительность ЦСС, определяемая средней интенсивностью выходного трафика; T – средняя временная задержка пакета в системе; $T_{доп}$ – допустимая временная задержка, определяющая ограничение для доставки и хранения пакетов в ЦСС.

Применение выражения (6) к известной модели идеальной ЦСС в виде M взаимно независимых ОС без конфликтов, повторных передач и потерь пакетов, с максимальными характеристиками по передаче (интенсивность выходного трафика каждой j-той ОС $\gamma_{вых\,j}$ ограничивается пропускной способностью КС $C_{кан\,j}$) и хранению информации (количество ожидающих передачи пакетов N_j определяется емкостью буферных запоминающих устройств каждого УК $N_{j\,доп}$), используемой для оценки потенциальных возможностей системы по обеспечению информационного обмена. Поэтому было введено понятие максимальной удельной интегральной нагрузки ЦСС

$$P_{max} = \sum_{j=1}^{M} N_j \gamma_{вых\,j} = \sum_{j=1}^{M} N_{j\,доп} C_{кан\,j} \,. \qquad (6)$$

Значение реальной УИН ЦСС (5), всегда меньше максимальной (6) вследствие не оптимальности управления входным потоком и маршрутизации, конфликтов при реализации множественного доступа, ошибок и потерей пакетов, повторных передач и

т.д. Таким образом, сравнение УИН и показателя (6) позволяет оценить степень использования ЦСС своих потенциальных возможностей по обеспечению информационного обмена. Применение введенного обобщенного показателя УИН позволяет получить количественную оценку информационной эффективности ЦСС с одновременным учетом в итоговом значении возможностей системы по передаче и хранению информации.

Используя выбранный обобщенный показатель, сущность первого разработанного способа оценки эффективности информационного обмена в ЦСС с учетом информационных потерь может быть сформулирована следующим образом. За выбранный интервал времени наблюдения ΔT, через заданные интервалы измерений $\Delta T_{изм}$ измеряются параметры блоков устройств ввода, передачи, вывода информации и запоминающих устройств ЦСС, с помощью которых вычисляются значения текущей УИН P_i (5) и максимальной УИН P_{max} (6) ЦСС. Дополнительно за этот интервал времени измеряются параметры: блока устройств вывода информации в результате чего определяется среднее количество ошибочно принятых пакетов $N_{ош}$ в ЦСС; блоков запоминающих устройств, устройств ввода и передачи информации, с помощью которых находится среднее количество недоставленных пакетов $N_{нд}$; блока устройств передачи информации на основе чего определяется значение интенсивности потока повторных передач $\gamma_{пп}$. Затем вычисляется общее среднее количество потерь информационных пакетов (информационных потерь в системе)

$$N_{пот} = N_{ош} + N_{нд} \qquad (7)$$

и определяются удельные информационные потери в ЦСС согласно выражению

$$P_{потi} = N_{пот}\gamma_{пп}\Big|_{T \le T_{доп},\, C_{кан\,j}}, \qquad (8)$$

где $\gamma_{пп}$ – средняя интенсивность потока повторных передач, ограничиваемая пропускной способностью КС $C_{кан\,j}$.

На основе полученных удельных информационных потерь уточняются значения УИН P_i и в соответствии с формулой

$$P_{ИП\,i} = P_i - P_{потi}. \qquad (9)$$

находится УИН ЦСС с учетом информационных потерь $P_{ИП\,i}$. После чего полученное значение сравнивается с максимальной УИН для оценки степени снижения эффективности информационного обмена вследствие потерь информационных пакетов

$$\delta P_{ИП\,i} = \left(1 - \frac{P_{ИП\,i}}{P_{max}}\right) \cdot 100\%. \qquad (10)$$

Сущность полученного способа оценки поясняется следующим. Учет возникающих в процессе информационного обмена потерь пакетов путем дополнительного определения удельных информационных потерь ЦСС, согласно известным источникам [1, 8] и проведенным исследованиям, позволяет существенно повысить точность оценки УИН ЦСС. Это, в свою очередь, позволяет своевременно реагировать на изменения условий функционирования ЦСС для поддержания высокой эффективности информационного обмена в реальном масштабе времени [9].

Техническим результатом разработанного способа является повышение точности оценки УИН за счет измерения за выбранный интервал времени ΔT общего среднего количества потерянных пакетов и интенсивности потока повторных передач

путем определения на их основе удельных информационных потерь в ЦСС и уточнения с их помощью значений УИН ЦСС.

При описании ЦСС используется понятие объекта связи 1 (рисунок 1), состоящего из основных блоков:

2 – блок устройств ввода информации в систему связи (БУВИ);

3 – блок запоминающих устройств (БЗУ);

4 – блок устройств передачи информации (БУПИ);

5 – блок устройств вывода информации из системы связи (БУВВИ).

Кроме того, структурная схема реализации предлагаемого способа включает в себя:

6 – блок вычисления УИН (БВУИН);

7 – блок вычисления максимальной УИН (БВМУИН).

А также блоки измерителя-вычислителя 8 информационных потерь в ЦСС:

9 – блок измерения среднего количества ошибочно принятых пакетов (БИСКОПП);

10 – блок измерения среднего количества недоставленных пакетов (БИСКНП);

11 – блок измерения значения интенсивности потока повторных передач (БИЗИППП);

12 – блок вычисления общего среднего количества информационных потерь (БВОСКИП);

13 – блок вычисления удельных информационных потерь (БВУИП);

14 – блок вычисления УИН с учетом информационных потерь (БВУИНИП);

15 – блок вычисления снижения эффективности информационного обмена вследствие потерь информационных пакетов (БВСЭИОИП).

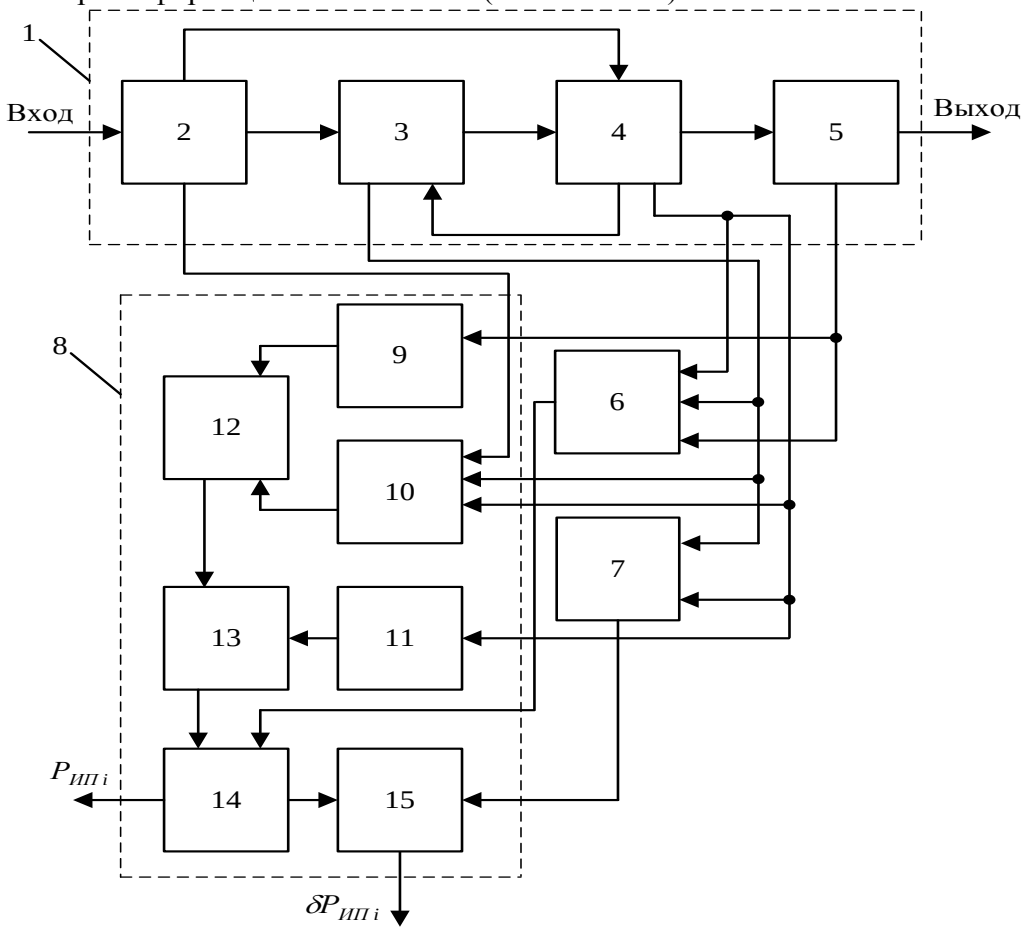


Рисунок 1 – Структурная схема реализации способа текущей оценки эффективности информационного обмена в ЦСС с учетом допустимых информационных потерь

Разработанный способ оценки эффективности информационного обмена в ЦСС, осуществляется следующим образом. Определение УИН P_i и максимальной УИН P_{max} системы производится по измерениям: емкостей каждого буфера БЗУ (блок 3) и количества информационных пакетов в ЦСС путем измерения занятых ячеек памяти каждого буфера БЗУ; суммарных пропускных способностей КС в БУПИ (блок 4) для каждого элемента БЗУ и производительности ЦСС путем измерения занятых ячеек памяти каждого буфера БУВВИ (блок 5); согласно известному способу [7] в БВУИН (блок 6) и БВМУИН (блок 7), соответственно. Дополнительно за выбранный интервал времени наблюдения ΔT, путем проведения заданного числа измерений n, определяются: среднее количество ошибочно принятых пакетов $N_{оп}$ в БИСКОПП (блок 9) на основе измерений ячеек памяти в БУВВИ (блок 5) ЦСС, освобождающихся вследствие формирования запросов на повторные передачи; среднее количество недоставленных пакетов $N_{нд}$ в БИСКНП (блок 10) на основе измерений количества освобожденных ячеек памяти буферов в БУВИ (блок 2), БЗУ (блок 3), и количества занятых ячеек памяти буферов в БУПИ (блок 4) ЦСС с учетом ограничения на $T_{доп}$; значение интенсивности потока повторных передач $\gamma_{пп}$ в БИЗИППП (блок 11) на основе измерений количества занятых ячеек памяти буферов пакетами с маркерами повторных передач в БУПИ (блок 4) ЦСС (например, с помощью счетчиков и делителей). Далее в БВОСКИП (блок 12), например, с использованием сумматора, производится операция сложения посчитанных значений $N_{оп}$ и $N_{нд}$ (выражение (7)), в результате чего определяется общее среднее количество информационных потерь (пакетов) в ЦСС $N_{пот}$. Далее в БВУИП (блок 13), например, с помощью перемножителя по формуле (8) осуществляется вычисление удельных информационных потерь ЦСС $P_{потi}$, с использованием которых в БВУИНИП (блок 14), например, с применением вычитающего устройства, уточняется значение УИН ЦСС и, согласно выражению (9), находится значение УИН ЦСС с учетом информационных потерь $P_{ИПi}$. После чего, по формуле (10) в БВСЭИОИП (блок 15), например, с помощью делителя, вычитающего устройства и перемножителя, вычисляется параметр $\delta P_{ИПi}$, характеризующий степень снижения эффективности информационного обмена вследствие потерь информационных пакетов в ЦСС.

Новизна предложенного способа состоит в том, что он позволяет учесть в параметре $P_{ИПi}$ характеристики информационных потерь ЦСС в процессе передачи информации, т.е. одновременно отразить влияние дестабилизирующих факторов на информационный обмен в ЦСС. В выражении (8) значение $N_{пот}$ определяет общее среднее значение потерянных пакетов в ЦСС за выбранный интервал времени ΔT, а $\gamma_{пп}$ значение интенсивности потока повторных передач, осуществляемых системой для обеспечения требований по своевременности и достоверности информационного обмена. Таким образом, уточненное значение УИН $P_{ИПi}$, определяет информационные потери ЦСС как в процессе хранения, так и передачи информации (в том числе повторных передач). Основным достоинством получаемой оценки является четкий физический смысл параметра, подтверждаемый тривиальными расчетами и измерениями. Кроме того, параметр $\Delta P_{ИПi}$ позволяет дополнительно оценить снижение эффективности информационного обмена в ЦСС по сравнению с максимальной УИН, вследствие потерь информационных пакетов.

Таким образом, разработанный способ позволяет уточнить оценку эффективности информационного обмена в ЦСС с учетом наличия информационных потерь за выбранный интервал времени. Он может быть использован при создании новых и совершенствовании существующих ЦСС на этапе получения адекватной оценки их функционирования с учетом воздействия дестабилизирующих факторов. Доказательством технической реализуемости полученного способа оценки информационного обмена в ЦСС, является то, что для его осуществления требуются стандартные элементы микроэлектроники, существующие средства измерительной и вычислительной техники, например, такие как: счетчики, сумматоры, перемножители, вычитающие устройства и делители, а также программное обеспечение, основой которого являются элементарные математические операции.

Способ интервальной оценки эффективности информационного обмена в ЦСС с учетом информационных потерь. Как было отмечено во вводной части работы, в условиях существенных изменений интенсивности входного трафика и воздействия дестабилизирующих факторов на ЦСС, необходим переход от точечных к интервальным оценкам эффективности информационного обмена с целью определения области высокой информационной эффективности системы по заданному критерию. Поэтому был разработан способ интервальной эффективности информационного обмена в ЦСС с учетом информационных потерь.

Разработанный способ практически реализуется путем измерений за выбранный интервал времени наблюдения ΔT, через заданные интервалы измерений $\Delta T_{изм}$ в блоках модели ЦСС (рисунок 1): БУВИ, БЗУ, БУПИ, БУВВИ, обеспечивающих определение в блоке измерителя-вычислителя интервала эффективной работы ЦСС (БИВИЭР) – полосы пропускания системы по входному трафику $[\gamma_{вх\,пор1}, \gamma_{вх\,пор2}]$ на заданном пороговом уровне УИН $P_{пор}$ [10]. После чего, для текущих значений интенсивности входного трафика $\gamma_{вх\,i}$ в промежутке от $\gamma_{вх\,пор1}$ до $\gamma_{вх\,пор2}$ через $\Delta T_{изм}$ производятся последовательные измерения: количества поступающих пакетов в БУВИ; количества пакетов, находящихся в БЗУ, и производительности ЦСС в БУВВИ системы, на основе которых вычисляются текущие значения приращений УИН по входному трафику и его пороговое значение, соответственно

$$D_{P_i} = \frac{P_{ИПi} - P_{ИПi-1}}{\gamma_{вх\,i} - \gamma_{вх\,i-1}} = \frac{\Delta P_{ИПi}}{\Delta \gamma_{вх\,i}}, \qquad (11)$$

$$D_{P_{пор}} = \frac{\Delta P_{ИП\,пор}}{\Delta \gamma_{вх\,пор}}, \qquad (12)$$

где $\Delta P_{ИПi}$ и $\Delta \gamma_{вх\,i}$ – текущие приращения УИН и входного трафика на i-том шаге измерений, соответственно; $\Delta P_{ИП\,пор} = 0{,}01 \cdot P_{ИПi}$ – пороговое значение приращения УИН с учетом появления в ЦСС информационных потерь, $\Delta \gamma_{вх\,пор} = M \cdot \Delta \gamma_{вх\,min}$ – пороговое значение приращения интенсивности входного трафика, определяемое $\Delta \gamma_{вх\,min}$ – минимальным приращением входного трафика в каждом КС на 1 пакет/с с заданным количеством M каналов при котором потери информационных пакетов не превышают $I_{пот} \le 1\%$ [1, 8].

При этом каждое значение D_{P_i} сравнивается с пороговым $D_{P_{пор}}$, и если

$$D_{P_i} > D_{P_{пор}}, \qquad (13)$$

то описанные выше действия продолжаются пока не выполнится условие $D_{P_i} \le D_{P_{пор}}$, после чего измерения и вычисления прекращаются. При этом фиксируется текущее значение интенсивности входного трафика $\gamma_{вх\,i} = \gamma_{вх\,пор\,D}$, и принимается решение о том, что ЦСС будет работать эффективно с обеспечением допустимого уровня информационных потерь в интервале входного трафика $П_{\gamma(D)} = [\gamma_{вх\,пор1}, \gamma_{вх\,пор\,D}]$, где $\gamma_{вх\,пор\,D}$ – верхняя граница интервала эффективной работы ЦСС при допустимом уровне информационных потерь (См. Рис. 2).

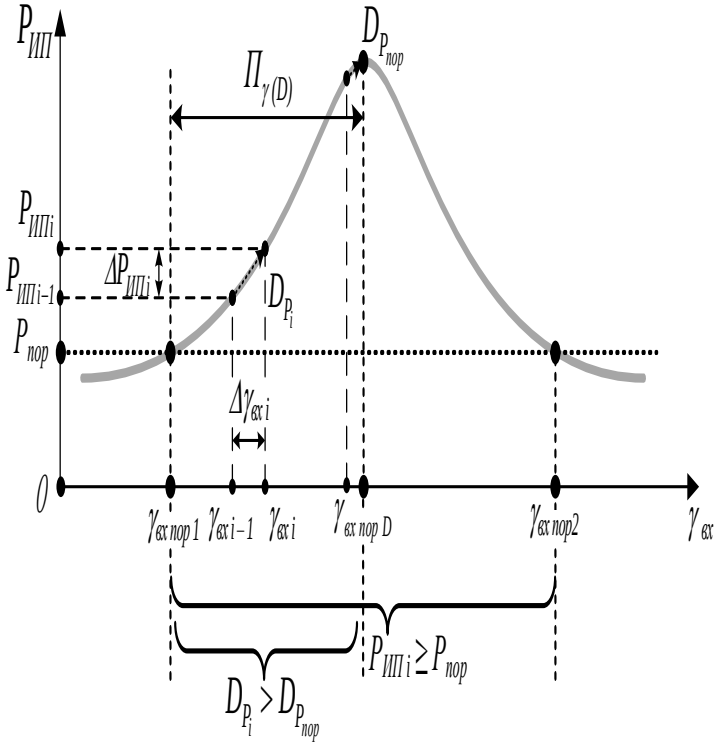


Рисунок 2 – Иллюстрация работы полученного способа интервальной оценки

Сущность разработанного способа интервальной оценки эффективности информационного обмена в ЦСС поясняется следующим. Проведение последовательных измерений текущих значений интенсивности входного трафика, УИН и ее приращений при изменении интенсивности входного трафика в интервале эффективной работы ЦСС (полосы пропускания) [10] позволяет определить интервал изменения входного трафика, в котором система функционирует с требуемой эффективностью информационного обмена при допустимом уровне информационных потерь с учетом требований по потерям информационных пакетов, указанных в рекомендациях Международного союза электросвязи [8]. В результате слева полоса пропускания ЦСС с учетом допустимых информационных потерь ограничивается в соответствии с заданным пороговым значением УИН значением входного трафика $\gamma_{вх\,пор1}$, полученным при определении интервала эффективной работы ЦСС [10], а справа – $\gamma_{вх\,пор\,D}$, которое определяется путем проверки неравенства (13) и ограничивается пороговым значением $D_{P_{пор}}$.

При описании ЦСС, аналогично способу оценки информационной эффективности с учетом информационных потерь представленному в предыдущем пункте работы (См. Рис. 1) используется понятие объекта связи 1 (рисунок 3), состоящего из основных блоков: 2 – БУВИ; 3 – БЗУ; 4 – БУПИ; 5 –БУВВИ.

Кроме того, структурная схема реализации данного способа включает в себя блоки:

6 – блок измерителя-вычислителя интервала эффективной работы ЦСС (БИВИЭР);

7 – блок сравнения входного трафика и управления (БСВТУ);

8 – блок измерителя-вычислителя приращения УИН (БИВП);

9 – блок измерителя-вычислителя порогового значения приращения УИН (БИВПЗП);

10 – блок сравнения приращения и управления (БСПУ);

11 – блока фиксации пороговых значений входного трафика (БФПЗВТ).

Способ оценки эффективности информационного обмена ЦСС с учетом информационных потерь осуществляется следующим образом (См. Рис. 3).

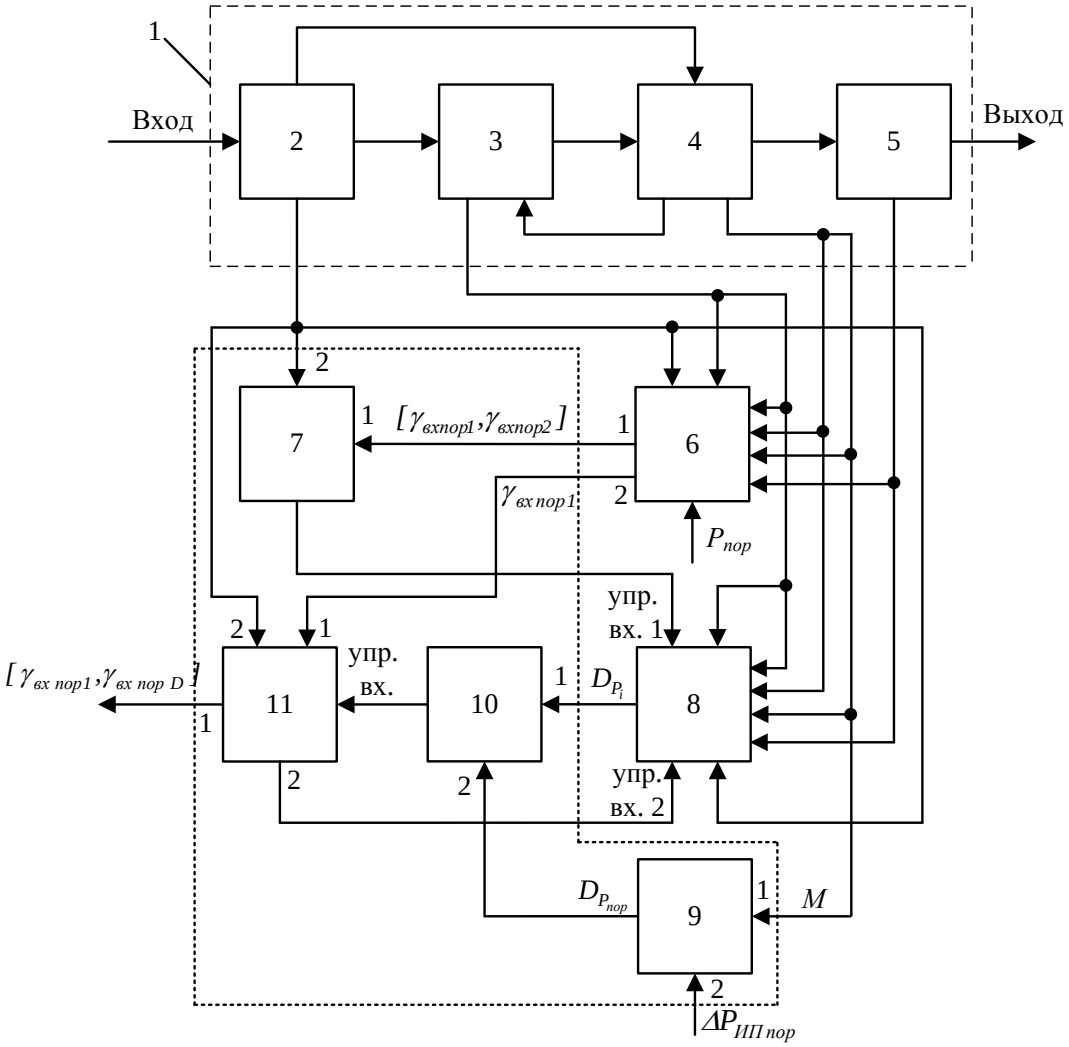


Рисунок 3 – Структурная схема реализации способа интервальной оценки информационной эффективности ЦСС с учетом допустимых информационных потерь

За выбранный интервал времени наблюдения ΔT, через заданные интервалы измерений $\Delta T_{изм}$ на основе последовательных измерений в блоках ЦСС: БУВИ (блок 2), БЗУ (блок 3), БУПИ (блок 4) и БУВВИ (блок 5) в БИВИЭР (блок 6) определяются текущие значения УИН $P_{ИП\,i}$ и сравниваются их с пороговым $P_{пор}$, в результате чего по известному способу [10] определяется интервал эффективной работы ЦСС по входному трафику $[\gamma_{вх\,пор1},\gamma_{вх\,пор2}]$, нижнее значение которого $\gamma_{вх\,пор1}$ направляется с выхода 2 БИВИЭР (блок 6) на вход 1 БФПЗВТ (блок 11), выполненного, например, в виде

запоминающего устройства, для его запоминания. Граничные значения интервала эффективной работы ЦСС $[\gamma_{вх\,пор1}, \gamma_{вх\,пор2}]$ с выхода 1 БИВИЭР (блок 6) подаются на вход 1 БСВТУ (блок 7), выполненного, например, в виде компаратора, для сравнения их с текущим значением интенсивности входного трафика $\gamma_{вх\,i}$, поступающим из БУВИ (блок 2) на вход 2 блока БСВТУ (блок 7). Если условия $\gamma_{вх\,пор1} \le \gamma_{вх\,i} \le \gamma_{вх\,пор2}$ не выполняются, то на выход БСВТУ (блок 7) управляющий сигнал не выдается. Иначе, на выходе БСВТУ (блок 7) формируется управляющий сигнал, который подается на управляющий вход (упр. вх. 1) БИВП (блок 8) для проведения измерений и вычислений через заданный интервал времени $\Delta T_{изм}$ текущих значений приращений УИН по входному трафику D_{P_i} на основе последовательных измерений в блоках: БУВИ (блок 2), БЗУ (блок 3), БУПИ (блок 4) и БУВВИ (блок 5) ЦСС. Далее из БУПИ (блок 4) на вход 1 БИВПЗП (блок 9) подается посчитанное количество КС M, а на вход 2 БИВПЗП (блок 9) – пороговое приращение УИН с учетом допустимых информационных потерь в ЦСС $\Delta P_{ИП\,пор}$, где, например, с помощью делителя определяется пороговое значение приращения УИН по входному трафику $D_{P_{пор}}$. Затем значения D_{P_i} из БИВП (блок 8) и $D_{P_{пор}}$ из БИВПЗП (блок 9) направляются, соответственно на входы 1 и 2 БСПУ (блок 10), выполненного, например, в виде компаратора, для их сравнения. При выполнении условия (13) на выход БСПУ (блок 10) управляющий сигнал не выдается и продолжаются измерения текущих значений приращений УИН по входному трафику D_{P_i}. Иначе, на выходе БСПУ (блок 10) формируется управляющий сигнал, который подается на управляющий вход (упр. вх.) БФПЗВТ (блок 11) и фиксируется текущее значение $\gamma_{вх\,i} = \gamma_{вх\,пор\,D}$, поступающее из БУВИ (блок 2) на вход 2 БФПЗВТ (блок 11). Далее с выхода 2 БФПЗВТ (блок 11) управляющий сигнал направляется на управляющий вход (упр. вх. 2) БИВП (блок 8) на прекращение измерений и вычислений через заданный интервал времени $\Delta T_{изм}$ текущих значений приращений УИН по входному трафику D_{P_i}. После чего на выход 1 БФПЗВТ (блок 11) выдаются граничные значения интервала интенсивностей входного трафика $П_{\gamma(D)} = [\gamma_{вх\,пор1}, \gamma_{вх\,пор\,D}]$ – полоса пропускания ЦСС с учетом допустимых информационных потерь.

Новизна предложенного способа состоит в том, что он обеспечивает определение интервала изменения интенсивности входного трафика, в пределах которого функционирование ЦСС осуществляется с требуемой эффективностью информационного обмена, оцениваемой значениями УИН, при одновременном обеспечении допустимого уровня информационных потерь, характеризуемого значениями приращений УИН по входному трафику.

Доказательством технической реализуемости разработанных способов является то, что все представленные выше операции для их осуществления могут быть выполнены на базе стандартных элементов микроэлектроники и быстродействующих микроконтроллеров с использованием программное обеспечение, основой которого являются элементарные математические операции.

Заключение. Выводы по работе. Таким образом, поставленную цель исследований можно считать достигнутой. На основе достаточно глубокого анализа известных подходов к оценке эффективности информационного обмена в ЦСС сформулирована актуальность оценивания функционирования системы в условиях изменения входного трафика и воздействия дестабилизирующих факторов с учетом

допустимых информационных потерь. Произведен обоснованный выбор обобщенного показателя – УИН ЦСС, одновременно характеризующего возможности передачи и хранения информации в системе. Разработаны способы текущей и интервальной оценки информационной эффективности, позволяющие, соответственно, уточнить значение обобщенного показателя и получить интервал эффективной работы ЦСС (полосу пропускания) при поддержании допустимых потерь информационных пакетов в системе $I_{пот} \le 1\%$. Представленные способы текущей и интервальной оценки эффективности информационного обмена в ЦСС с учетом информационных потерь могут быть практически реализованы на существующей элементной базе и применены при решении задач адекватной оценки информационной эффективности и адаптации ЦСС в условиях изменения входного трафика и воздействия дестабилизирующих факторов [9].

Перечень используемой литературы и источников:

1. Назаров А.Н. Модели и методы расчета показателей качества функционирования узлового оборудования и структурно-сетевых параметров сетей связи следующего поколения / А.Н. Назаров, К.И. Сычев. – Красноярск: Изд-во Поликом, 2010. – 389 с.
2. Kleinrock L. Queueing Systems: Problems and Solutions / L. Kleinrock, R. Gail // Wiley-Interscience, 1996. – 240 p.
3. Bertsekas, D. Data Networks: 2nd ed. / D. Bertsekas, R. Gallager // Prentice-Hall, Englewood Cliffs. NJ, 1992. – 556 p.
4. Головин О.В. Системы и устройства коротковолновой радиосвязи / О.В. Головин, С.П. Простов. – Москва: Горячая линия – Телеком, 2006. – 600 с.
5. Карганов В. В. Показатель оценки эффективности систем связи и их элементов связи / В.В. Карганов, А.Г. Расчесова, В.А. Кудряшов // Научно-технические ведомости СПб ГПУ. – 2016. – №1. – С. 7-14.
6. Шаров А.Н. Сети радиосвязи с пакетной передачей информации / А.Н. Шаров, В.А. Степанец, В.И. Комашинский. – СПб.: ВАС им. С.М. Буденного, 1994. – 216 с.
7. Межуев А.М. Оценка эффективности сетевых информационных систем обобщенным показателем / А.М. Межуев, А.В. Коренной // Радиотехника. – 2021. – № 3. – С. 65-77.
8. Recommendation E.802. Overall network operation, telephone service, service operation and human factors // Введ. 2007-02-08. – МСЭ-Т, 2007. – 37 с.
9. Межуев А.М. Структурная адаптация телекоммуникационных систем с обеспечением допустимых информационных потерь / А.М. Межуев, А.В. Коренной, Д.Л. Стуров // Радиотехника. – Москва. – 2020. – № 3(5). – С. 29 – 39.
10. Патент №2571917 Российская Федерация. МПК7 H 04 L 29/00. Способ оценки эффективности информационного обмена системы связи / Межуев А.М., Пасечников И.И., Роговенко О.Н.; заявитель и патентообладатель ВУНЦ ВВС «ВВА». № 2014140578/08; заявл. 07.10.2014; опубл. 27.12.2015, Бюл. № 36. – 3с.

1.6. СИСТЕМА УПРАВЛЕНИЯ ОБНАРУЖЕНИЕМ КОМПЬЮТЕРНЫХ АТАК НА БАЗЕ НЕЙРО-НЕЧЕТКОЙ ЛОГИКИ В КРИТИЧЕСКОЙ ИНФОРМАЦИОННОЙ ИНФРАСТРУКТУРЕ

С развитием информационно-коммуникативной сферы вопрос защиты информации становится с каждым днем все актуальное и важнее в различных сферах деятельности. Поэтому в данной статье автор рассматривает систему обнаружения компьютерных атак на базе нейро-нечеткой логики.

Ключевые слова: информационная безопасность, компьютерные атаки, нейро-нечетная логика, объекты критической информационной инфраструктуры (КИИ), система управления обнаружением компьютерных атак.

COMPUTER ATTACK DETECTION CONTROL SYSTEM BASED ON NEURAL-FUZZY LOGIC IN CRITICAL INFORMATION INFRASTRUCTURE

With the development of the information and communication sphere, the issue of information security is becoming more relevant and more important every day in various fields of activity. Therefore, in this article the author considers a system for detecting computer attacks based on neuro-fuzzy logic.

Key words: information security, computer attacks, neuro-odd logic, critical information infrastructure objects (CII), computer attack detection management system.

Новые разновидности компьютерных атак, в т.ч. полиморфные целевые атаки, атаки на динамическую маршрутизацию, туннельные атаки, сложно определяются либо вовсе не определяются при помощи традиционных методов обнаружения и могут приводить не только к нарушениям конфиденциальности, целостности и доступности информационных ресурсов, но и к нарушениям непрерывного функционирования объектов критической информационной инфраструктуры (КИИ) [1, 2]. Критическим становится противоречие между вариативностью действующих атак, скоростью их реализации и инертностью механизмов обнаружения, что ослабляет защищенность значимых объектов КИИ, используемых в банковской сфере, в системах транспорта, связи, энергетики, атомной и химической промышленности, а также усиливает социальные и техногенные риски [3].

Для решения проблем, связанных с недостатком информации, необходимой для получения количественного описания протекающих в системе процессов, так и сложностью объекта управления, предлагается использовать аппарат нечеткой логики. Теория нечетких множеств позволяет строить нечеткие модели объектов с использованием лингвистических переменных и механизмов логического вывода [4]. В настоящее время модели нечеткого логического вывода используются при разработке нечетких экспертных систем, применяемых для решения задач диагностики, управления, поддержки принятия решений в различных предметных областях.

В данной работе представлена система управления обнаружением компьютерных атак на объекты КИИ, реализующая выбор детекторов атак в режиме реального времени, за счет комбинирования искусственных нейросетей и аппарата нечеткой логики. Также определена структура базы знаний, и предложен комплекс новых методов обнаружения компьютерных атак, покрывающих множество актуальных киберугроз объектам КИИ.

Для обеспечения гибкости при формировании базы знаний предлагается использовать модифицированные нечеткие продукционные правила, формулируемые в виде нечетких высказываний относительно значений тех или иных лингвистических переменных. В рамках решаемой задачи в качестве анализируемых данных предлагается набор характеристик объекта защиты: сетевые параметры, доступные вычислительные ресурсы для работы системы анализа киберугроз, экономические показатели, допустимое время реакции на компьютерную атаку, а также текущий уровень киберугроз. Собранные данные необходимо предобработать и преобразовать в базу методов обнаружения компьютерных атак следующей структуры (См. Таб. 1).

Таблица 1 – Структура базы методов обнаружения компьютерных атак

Входные переменные										**Выходная переменная**
Сетевые характеристики		**Вычислительные ресурсы**			**Экономические параметры**	**Время реакции**	**Уровень киберугроз**		**Параметры типов атак**	**Методы обнаружения атак**
Кол-во узлов	*Скорость передачи данных*	*ЦП*	*ОП*	*Диск*	*Стоимость активов*	*Временные задержки*	*DoS-атак*	*Черная дыра*	*Активное воздействие*	*Нейросетевой метод*
Н	Н	Н	Н	Н	Н	Н	Н	Н	Н	*Метод машинного обучения*
С	С	С	С	С	С	С	С	С	С	*Роевой интеллект*
В	В	В	В	В	В	В	В	В	В	*Метод выравнивания*

Для каждого из признаков определено терм-множество вида {Н (низкий), С (средний), В (высокий)}, а также задана функция принадлежности, ставящая в соответствие значению терм.

Предложенная структура поддерживает расширение характеристик объекта, обнаруживаемых компьютерных атак и детекторов. Добавление новой информации в

базу знаний может осуществляться вручную оператором системы управления или за счет самообучения системы (приспособления к новым условиям или задачам).

Для принятия решений в условиях неполноты знаний об объекте защиты и актуальных киберугрозах реализована нейро-нечеткая модель, основанная на адаптивной системе нейро-нечеткого вывода ANFIS на базе алгоритма Такаги-Сугено-Канга, основным преимуществом которого является высокая производительность и точность. Данная нечеткая адаптивная сеть базируется на следующих положениях: входные переменные являются четкими, функции принадлежности всех перечисленных множеств определены функцией Гаусса.

Перечень использованной литературы и источников:

1. Cho H., Lim S., Belenko V., Kalinin M., Zegzhda D., Nuralieva E. Application and improvement of sequence alignment algorithms for intrusion detection in the Internet of Things. In 2020 IEEE Conference on Industrial Cyberphysical Systems (ICPS). – 2020. Vol. 1. pp. 93-97.

2. Lim S., Kalinin M., Zegzhda P. Bioinspired Intrusion Detection in ITC Infrastructures. In International Conference on Technological Transformation: A New Role for Human, Machines and Management. Springer, Cham. – 2020. pp. 10-22.

3. Овасапян Т. Д. Применение нейронных сетей для выявления внутренних нарушителей в VANET-сетях / Т.Д. Овасапян, Д.А. Москвин, М.О. Калинин // Проблемы информационной безопасности. Компьютерные системы. – 2018. – № 1. – С. 68-73.

4. Катасев А.С. Методы и алгоритмы формирования нечетких моделей оценки состояния объектов в условиях неопределенности / А.С. Катасев // Вестник Технологического университета. – 2019. – Т. 22. – № 3. – С. 138-147.

1.7. ОНЛАЙН КОМПИЛЯЦИИ КОДА АГЕНТОВ НА ПЛАТФОРМЕ IACPAAS

В работе даётся цель и детали реализации компиляции кодов программных агентов на платформе IACPaaS. Описана реализация компонентов решателя «Редактор агентов», применяемого для их декларативной спецификации, редактирования исходного и построения исполняемого кода.

Ключевые слова: облачные вычисления, компиляция, код, «Java», IACPaaS.

ONLINE COMPILATION OF AGENT CODE ON THE IACPAAS PLATFORM

The paper presents the purpose and implementation details for the compilation of software agent codes on the IACPaaS platform. The implementation of the components of the «Agent editor» solver used for agent declarative specification, source code editing and executable code construction is described.

Keywords: cloud computing, compilation, code, "Java", IACPaaS.

Введение. Современный этап развития области создания программного обеспечения открывает перед разработчиком широкие возможности. Сейчас можно выбирать, где хранить данные программ, сами программы, а также их исходный код – локально или в удалённых средах. Для расширения круга пользователей и повышения удобства использования появились «облачные» хранилища данных, веб-сервисы, а для облегчения труда разработчиков – многопользовательские системы хранения версий исходного кода. При этом обычно создание рабочего кода из исходного (и, при возможности, отладка) всё ещё производится на оборудовании разработчика, после чего рабочая версия приложения отправляется в среду исполнения, а исходный код – в репозиторий, и эти сущности хранятся независимо.

В некоторых экосистемах исходный код может представлять ценность не только для тех разработчиков, которые его создают, но и для прочих – при повторном использовании. Кроме того, может происходить смена владельца или сопроводителя приложения. Наличие единой облачной инфраструктуры, которая поддерживала бы хранение исходного кода как можно «ближе» к работающему приложению может облегчить поддержку приложения в таких ситуациях. А присутствие в такой среде

подсистемы построения рабочего кода из исходного упрощает/ускоряет получение обновлённых версий приложения.

Проблемы работы с кодом в исходной реализации платформы IACPaaS. Основная задача, решаемая онлайн компиляцией исходного кода на платформе, состоит в обеспечении соответствия исходного кода и байт-кода (на платформе используется язык «Java»). Изначальная реализация облачной платформы IACPaaS [1] позволяла хранить на платформе только исполняемый код (получаемый разработчиком на собственном оборудовании), а исходный, формируемый также на оборудовании разработчиков, мог быть загружен ими в платформу лишь по желанию. Опыт использования платформы показал, что при этом затрудняется полная поддержка жизненного цикла агентов ввиду того, что, несмотря на наличие возможностей по загрузке исходного кода, разработчики выполняют только загрузку байт-кода. При прекращении разработчиком программной единицы работы с платформой (но передаче агентов в собственность другим пользователям) теряется возможность доработки и модификации созданных им агентов – исходного кода нет (он обычно остается только у ушедшего разработчика). Использование декомпиляторов байт-кода в исходный код не является удобным решением, которое следовало бы использовать на постоянной основе. Наиболее простой путь побуждения к загрузке исходного кода на платформу – заменить загрузку байт-кода на загрузку исходного кода и организовать средства получения рабочего кода на самой платформе. При этом устраняется и вторая проблема поддержки жизненного цикла – возможное несоответствие байт-кода и исходного кода (в случае наличия многих версий последнего). Ещё одно преимущество – повышение скорости разработки (нет необходимости выполнять два отдельных шага по загрузке – для исходного и для байт- кодов). Таким образом, введение онлайн компиляции исходного кода является задачей, решение которой позволяет лучше поддержать жизненный цикл программных единиц без увеличения числа действий, выполняемых разработчиком.

Этапы реализации онлайн компиляции агента.

1) модификация мета-информационного ресурса «Структура агента»;

2) модификация элементов решателя задач «Редактор агентов», разработанного по технологии [2]:

а) модификация ресурса «таблица соответствий»;

б) разработка агента, отвечающего за создание исходного кода;

в) модификация агента, играющего роль менеджера кода: вместо байт-кода он должен получать исходный код, оправлять его на компиляцию, затем (как уже заведено) отправлять байт-код на проверку, а затем, при необходимости, – сохранять его в ресурс агента в качестве исполняемого;

г) разработка агента, выполняющего компиляцию исходного кода, с выдачей байт-кода или сообщения об ошибке.

Структура агента. Данный системный ресурс содержит подграф, позволяющий хранить в целевой информации коды агента:

```
Структура агента {
 ~copymm ~new исходный код {
  ~seq версия { #авто-именование 1-2-3-...
   ~new системный код { ~new код [blob] }
   ~new собственный код { ~new -> код; }
  }
  ~clone текущая версия [str] #клон от «версия»
 }
 ~copymm ~new исполняемый код {
  ~new системный байткод { ~list ~new байткод [blob] }
```

~new собственный байткод {~list ~new байткод [blob]}
~copymm ~new ["загрузить"]
} }

Модификация данной структуры состоит в удалении вершины «загрузить», которая являлась командной и служила для загрузки исполнимого байт-кода в платформу с ПК разработчика. Также в подграфе «исходный код» введена вершина «версия», порождения по которой принимают значения из натурального ряда (а в комментарии к данным вершинам может храниться описание версий). Для указания текущей версии, по которой получается исполняемый код, введена вершина «текущая версия», которая должна создаваться зависимым клоном от некоторой вершины с метапонятием «версия».

Таблица соответствия для редактора агентов. Наиболее важная её модификация состоит в изменении соответствия *1*. Здесь вместо агента, выполняющего загрузку исполнимого кода, теперь описывается обращение к агенту, выполняющему формирование исполняемого кода из версии исходного кода, соответствующей «текущей».

Также были созданы новые соответствия, которые специфицируют взаимодействие с агентами при редактировании исходного кода:

- вызов агента для отображения формы описания и последующего сохранения новой версии исходного кода (предусмотрено два режима: из заготовки, формируемой по декларативному описанию, и в виде копии уже существующей версии);

- вызов агента для отображения формы редактирования исходного кода и выполнения команд, поступающих от управляющих элементов этой формы (сохранение кода, проверка компиляции, возврат к заготовке, откат изменений, скачивание, загрузка (См. Рис. 1);

- вызов агента для диалогового выбора и сохранения текущей версии.

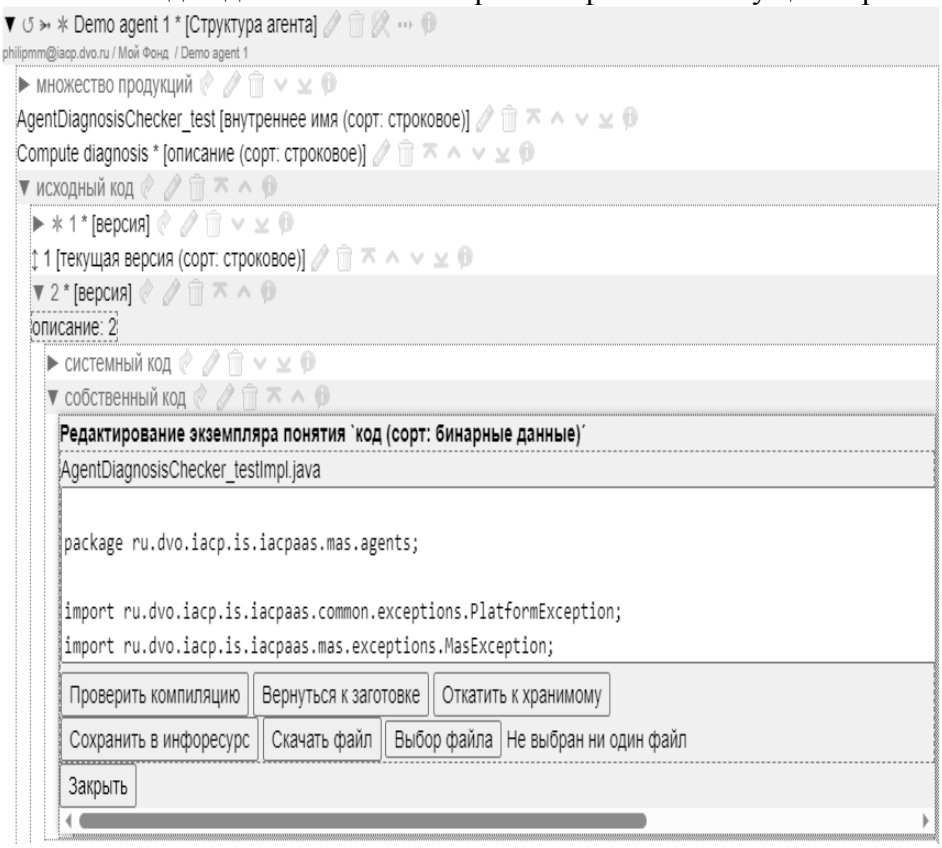


Рисунок 1 – Интерфейс формы редактирования исходного кода в Редакторе агентов.

Агент для работы с исходным кодом. Этот агент разработан по технологии [2] и, в частности, ответственен за интерфейс рис.1. При любом изменении исходного кода, являющегося текущей версией, и сохранении этих изменений – агент удаляет исполняемый код. Его необходимо получить заново, чтобы агент вновь стал рабочим – тем самым обеспечивается соответствие байт-кода и исходного кода.

Агент для формирования-проверки-сохранения исполняемого кода. Его разработка выполнена согласно одному из этапов технологии [2]. Это этап разработки агента, к которому будет обращаться агент интерфейсный контроллер Редактора агентов. Его разработка, в частности, схожа с разработкой других агентов, подключенных к решателю через таблицу соответствий, например, агент, отвечающих за проверку уникальности и установку внутреннего имени агента.

Агент для компиляции исходного кода. Данный агент вызывается по клику на командной мета-вершине «исполняемый код». Последовательность его работы следующая (интерфейсы – См. Рис. 2):

- отображение интерфейса для инициации компилирования кода,
- при инициации компиляции – извлечение исходного кода текущей версии и последовательная раздача заданий: а) компиляция, б) проверка безопасности байт-кода, в) сохранение байт-кода как исполняемого или отображение сообщения о возникшей ошибке.

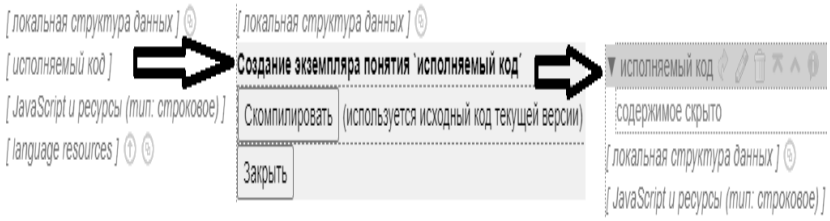


Рисунок 2 – Этапы создания исполняемого кода в Редакторе агентов.

Для получения исходного кода использована компиляция через командную строку, выполняющаяся в создаваемой временной папке:

- из указанной версии исходного кода агента извлекаются значения вершин с мета-вершиной «код», расположенных под вершинами «системный код» и «собственный код», и сохраняются в созданную папку в виде java файлов, туда же помещается jar файл с API платформы;
- вызывается команда компиляции с выводом ошибок в файл: javac -Xmaxerrs 1 -classpath "iacpaas-api-1.0.jar" "agent.java" "agentImpl.java" 2> "errors.txt";
- при наличии текста ошибки компиляции в файле errors.txt – возвращается этот текст, а в противном случае – возвращается содержимое всех полученных class-файлов с байт-кодом.

Перечень использованной литературы и источников:

1. Грибова В.В., Москаленко Ф.М., Тимченко В.А., Шалфеева Е.А. Платформа IACPaaS для разработки систем на основе онтологий: десятилетие использования // Искусственный интеллект и принятие решений. – 2022. - № 4. – С 55-65.

2. Грибова В.В., Клещев А.С., Москаленко Ф.М., Тимченко В.А., Федорищев Л.А., Шалфеева Е.А., Управляемая графовыми грамматиками разработка оболочек интеллектуальных сервисов на облачной платформе IACPaaS // Программная инженерия. – 2017. - №10. – С. 435-447.

1.8. ПРОШЛОЕ И НАСТОЯЩЕЕ ШИФРОВАНИЯ ИНФОРМАЦИИ, В КОНТЕКСТЕ ОБЕСПЕЧЕНИЯ ИНФОРМАЦИОННОЙ БЕЗОПАСНОСТИ

Современное общество принято называть – «информационным». Широкое развитие средств вычислительной техники и связи позволяет собирать, хранить, обрабатывать и передавать информацию в таких объемах и с такой оперативностью, которые были немыслимы раньше. Но при этом возник вопрос: «А, как защитить информацию?». Этот вопрос в человеческом обществе (прежде

всего в государственных структурах) стоял как в прошлом, так и настоящем. Поэтому в данной статье, мы кратко рассмотрим некоторые исторические этапы формирования систем обеспечения «информационной безопасности» в области шифрования (криптографии).
Ключевые слова: информация, информационная безопасность, криптосистема, «шифр Цезаря», шифры «Гронсфельда», «Виженера» и «Тримеуса».

PAST AND PRESENT OF INFORMATION ENCRYPTION, IN THE CONTEXT OF INFORMATION SECURITY

Modern society is usually called "informational". The widespread development of computer technology and communications makes it possible to collect, store, process and transmit information in such volumes and with such efficiency that were previously unimaginable. But the question arose: "How to protect information?" This question has arisen in human society (primarily in government structures) both in the past and present. Therefore, in this article, we will briefly consider some historical stages in the formation of systems for ensuring "information security" in the field of encryption (cryptography).
Key words: information, information security, cryptosystem, "Caesar cipher", "Gronsfeld", "Vigenere" and "Trimaeus" ciphers.

Шифры – это защита. Для современного человека это то же, что панцирь для черепахи, чернильный мешок для осьминога, маскировка для хамелеона. ... Защита информации – это закон жизни, одинаково непреложный и для государства, и для отдельного организма.

Девид Кан консультант Конгресса США
по вопросам криптографии

Исследователям истории связи известно, что первыми «шифровальщиками» в истории защиты информации были египтяне, которые еще во времена фараона Аменемхета II (1882–1872 до н.э.) приступили к расписыванию стен своих жилищ странными иероглифами. Их последователями были жители древней Месопотамии (одна из великих цивилизаций Древнего мира; наряду с Египтом считается первой на Земле; возникла в середине 4-го тысячелетия до н.э., угасла – в начале нашей эры), их дома украшали своеобразные и несущие в себе некий определенный смысл картинки. Далее последовали жители иудейского царства и греки, которые также придумывали необычные способы шифрования информации [1,3].

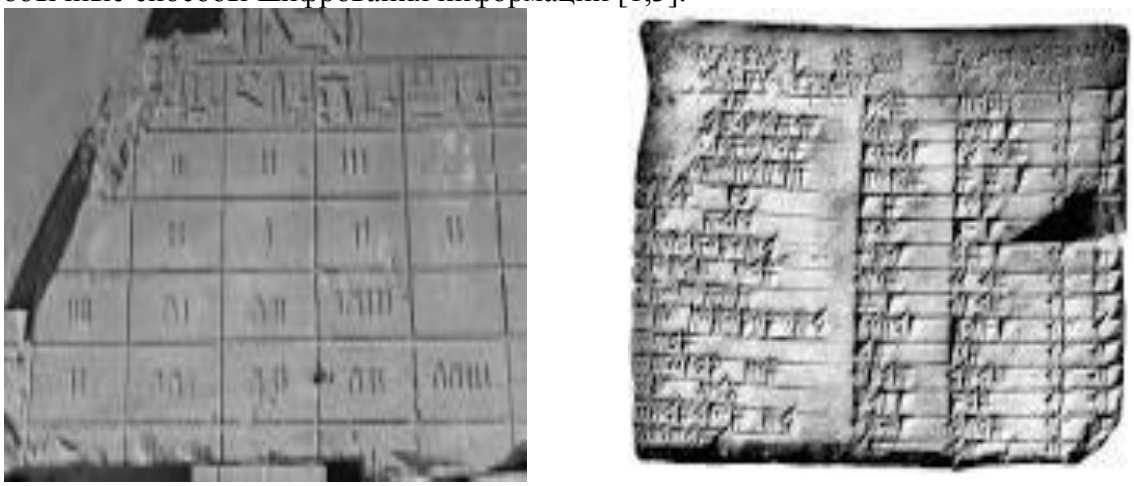


Рисунок 1 – Глиняные таблицы древних египтян месопотамцев

Но основателем зарождения шифрования информации (т.е. – криптографии) считается римский император Гай Юлий Цезарь (12.07.100 до н.э.- 5.03.44 до н.э.), который изобрел самый известный шифр – «шифр Цезаря» [9, 12, 15]. Сам Цезарь использовал этот шифр для ведения секретной переписки со своими военноначальниками в ходе военных действий, поскольку главная задача шифрования

информации – это ее сокрытие от третьих лиц. В настоящее время «шифр Цезаря» является самым простым при изучении основ криптографии и заключается в сдвиге на определенную позицию символа в алфавите. Т.е. в «шифре Цезаря» каждая буква в открытом тексте смещается на три позиции так, что буква «A», например, замещается буквой «D». Буква «B» замещается буквой «E» и так далее. Конец алфавита замыкается на его начало так, что буква «X» замещается буквой «A», а буква «Y» – буквой «B», «Z» – «C». В «шифре Цезаря» каждая буква смещается на 3 позиции, однако в более широком смысле этот шифр можно рассматривать, как смещение на некое целое число позиций (k), причем число k будет играть роль ключа.

Рисунок 2 - Схема преобразования,
выполняемое «шифром Цезаря»

С точки зрения современности «шифр Цезаря» считается моноалфавитной криптосистемой, которой на смену пришла полиалфавитная. Полиалфавитная криптосистема – это набор нескольких моноалфавитных систем, примерами которых являются: шифры «Гронсфельда» (создан в 1734 году бельгийцем Хосе де Бронкхором, графом Гронсвельдом) [13], «Виженера» (создан Джованни Баттиста Беллазо в 1553 году, однако в XIX веке получил имя Блеза Виженера, французского дипломата) [7] и «Тримеуса» [2]. Если в моноалфавитных криптосистемах сдвиг происходит на определенную позицию для всех символов в сообщении, то в полиалфавитных для каждого символа существует свой сдвиг – это усложняет задачу дешифрования информации [2].

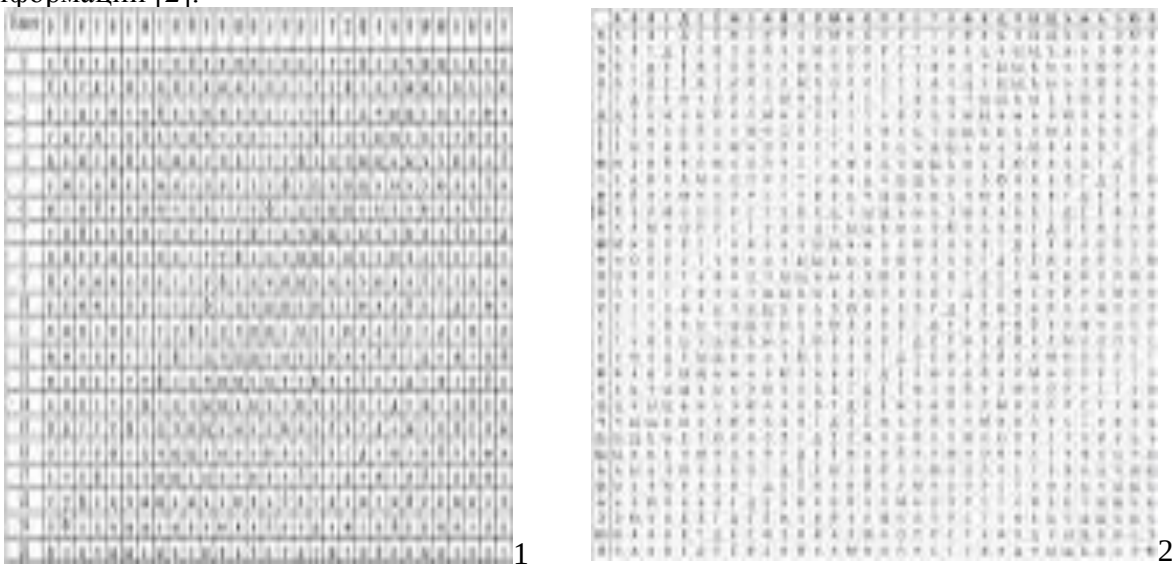


Рисунок 3 – Структура моноалфавитных систем шифров
1 - шифра «Гронсфельда»; **2** - шифр «Виженера»

С развитием систем шифрования появились такие понятия, как потоковые и блочные шифры:

1) В потоковых шифрах существует генератор псевдослучайных чисел, так как он отвечает за появление ключа.

2) В блочных шифрах весь исходных текст разбивается на блоки фиксированной длины, с каждым из которых ведется работа по отдельности, а затем все блоки складываются вместе и получается шифротекст.

Но у блочных шифров может быть два режима:

- *первый режим* – это простой замены, шифроблоки в котором являются независимыми, то есть при замене любого из блоков остальные не изменяются.

- *второй режим* – это сцепления блоков, последующие шифроблоки в котором зависят от предыдущего шифроблока.

Вся описанная нами к данному момента – система шифрования (криптография) подразумевала собой использование лишь одного ключа шифрования. С изобретением двухключевых систем, алгоритмы шифрования стали подразделяться на два вида:

- первый – *это симметричные, используемые один ключ (закрытый), который нужно как-то передать по закрытому каналу связи другому абоненту;*

- второй – *это ассиметричные, в которых используется два ключа – один открытый, используемый только для шифрования, а другой закрытый, используемый только для дешифрования* [11].

Примерами современных симметричных алгоритмов шифрования являются – «DES», «AES», «IDEA». Хоть они и являются современными, а два из последних используются и на сегодняшний момент, как выше упоминалось, они все являются одноключевыми системами, ключ которых нужно передать по закрытому каналу связи.

В определенный момент времени в области информационной безопасности стала задача о возможности передачи ключа шифрования по открытой линии связи. Поэтому в 1976 г. американский криптограф доктор технических наук Бейли Уитфилд Деффи совместно с профессором Мартином Эдвардом Хеллманом опубликовали научную работу, в исследовании которой был представлен алгоритм обмена ключами, позже названный «алгоритмом Диффи-Хеллмана». Суть данного алгоритма заключалось в том, что в ходе обмена некоторыми числами между абонентами по открытой линии связи и математических вычислений этих цифр, они смогли получить общий секретный ключ, который как раз можно использовать для шифрования любым из симметричных алгоритмов [12, 14].

Позже на концепции «алгоритма Диффи-Хеллмана» начали создаваться более сложные, такие как алгоритмы: «Шамира» (*Работа алгоритма основана на обратной нумерации линейный алгоритм отыскания минимального разрезающего контуры множества в сводимом управляющем графе. «Шамира» разработан в 1979 г. израильским учёным в области теории вычислительных систем, профессором информатики и прикладной математики НИИ имени Вейцмана в г. Реховот - Ади Шамиром*), «Эль-Гамаля» (*Криптосистема с открытым ключом, основанная на трудности вычисления дискретных логарифмов в конечном поле. Создана 1985 году американо-египетским специалистом в области защиты информации Тахером Эль-Гамалем*) и «RSA» (*Криптографических алгоритм с открытым ключом, основывающийся на вычислительной сложности задачи факторизации больших полупростых чисел. Криптосистема «RSA» стала первой системой, пригодной как для шифрования, так и для цифровой подписи. Создана сотрудниками Массачусетского технологического института (США) Роном Ривестом, Ади Шамиром и Леонардом Адлеманом*). Последний алгоритм в настоящее время является самым актуальным международным протоколом, используемым практически во всех информационных системах. Но у криптографии с открытым ключом есть одна большая проблема – невозможность подтверждения факта подлинности ключа, и чтобы ее решить была создана инфраструктура открытых ключей, в которой предполагается, что есть третья сторона, которой все доверяют.

Но помимо генерации общих секретных ключей и шифрования информации в современных системах защиты информации появился еще один криптографический примитив – аутентификация, т.е. – процедура проверки подлинности (MAC, HMAC) [6, 8]. Примеров аутентификации существует очень много, но на данный момент используется многофакторная аутентификация, которая включает в себя сразу несколько методов.

Одна из современных технологий обеспечения информационной безопасности является «VPN» или виртуальные частные сети, которые решают множество проблем не только информационной безопасности, но и конфиденциальности, поскольку множеству пользователей важно, чтобы при перехвате трафика нельзя было понять, чем он занимается в интернете. Трафик в «VPN» расшифровать невозможно, но существуют некоторые особенности, относящиеся к перехвату пакетов, которые могут идентифицировать использование «VPN» [6].

Существуют компании и целые страны, заинтересованные в запрете использования технологии VPN, поэтому в скором будущем станет возможным идентифицировать ее. Но поскольку есть и такие стороны, которым важно иметь возможность скрыть факт использования VPN встает вопрос о разработке метода скрытия.

В заключении мы можем сделать несколько выводов:

- первый: информационная безопасность в настоящее время может быть определена как система средств и способов по недопущению нанесения вреда свойствам различным объектам безопасности;

- второй: исходя из заявленной нами темы, что быть защитить объекты критической инфраструктуры необходимо на знаниях прошлого развивать новое.

Перечень использованной литературы и источников:

1. Бабаш А.В., Шанкин Г.П. История криптографии. В 2-х частях. Часть 1. / А.В. Бабаш, Г.П. Шанкин. – Москва: Издательство: Гелиос АРВ, 2002. – 240 с.
2. Грушо А.А., Тимонина Е.Е. Теоретические основы защиты информации. – Москва: Издательство Агентства «Яхтсмен». 1996. – 192с.
3. Девид Кан. Взломщики кодов / Пер. с англ.; Кан Девид. – Москва: Центрполиграф, 2000. – 480с. – (Серия «Секретная папка»).
4. Жельников В. Криптография от папируса до компьютера / В. Жельников. – Москва: ABF, 1996. – 335с.
5. Зюзин В.Д., Вдовенко Д.В., Большаков В.Н. Исследование HMAC на примере метода авторизации вызов-ответ // Современная наука: актуальные проблемы теории и практики. Серия: Естественные и технические науки. – 2020. – № 4. – С. 81-87.
6. Зюзин В.Д., Вдовенко Д.В., Большаков В.Н. Атака на хэш-функции // Евразийский журнал биологических наук, 2020. – № 1. – С. 907-913.
7. Морозенко В.В., Плешкова И.Ю. О применении генетического алгоритма для криптоанализа шифра Виженера/ В.В. Морозенко, И.Ю. Плешкова // Современные проблемы науки и образования: Сетевое издание. – 2014. - № 2. – URL: https://science-education.ru/ru/article/view?id=12321 (Дата обращения: 21.11.2023).
8. Насколько легко обнаружить использование VPN? [Электронный ресурс]. – URL: www.comparitech.com/blog/vpn-privacy/how-easy-is-it-to-detect-a-vpn (Дата обращения: 22.11.2023).
9. Протько М.А., Борисенко О.Ф. Шифр Цезаря и генетический алгоритм материалы / М.А. Протько, О.Ф. Борисенко // Компьютерные системы и сети: сборник статей 58-й научной конференции аспирантов, магистрантов и студентов БГУИР (Минск, 18–22 апреля 2022 г.). – Минск: Изд-во БГУИР, 2022. – С. 69-77.
10. Рябко Б.Я., Фионов А.Н. Криптографические методы защиты информации: Учебное пособие для вузов. – 2-е издание, стереотипное / Б.Я. Рябко, А.Н. Фионов. – Москва: Горячая линия - Телеком, 2012. – 229 с.
11. Санников В.Г. Введение в теорию и методы криптографической защиты информации: Учебное пособие / В.Г. Санников. – Москва: МТУСИ, 2009. – 98с.
12. Сингх Саймон. Книга шифров: Тайная история шифров и их расшифровки / Саймон Сингх; пер. с англ. А. Галыгина. – Москва: Издательство «АСТ», 2009. – 448с.
13. Шмалева К.А., Баянов И.Б. Шифр Гронсфельда с ключевым словом / К.А. Шмалева, И.Б. Баянов // Актуальные вопросы современной техники и технологии. Сборник докладов XXII Международной научной конференции. Отв. ред. А.В. Горбенко. – Липецк: Издательство: Научное партнерство «Аргумент», 2016. – С. 36-38.

14. Шмидт Э., Коэн Дж. Новый цифровой мир. Как технологии меняют жизнь людей, модели бизнеса и понятие государств: Пер. с англ. Сергея Филина. – Москва: Манн, Иванов и Фарбер, 2013. – 368 с.
15. Ясенев В.Н. Конспект лекций по информационной безопасности / В.Н. Ясенев. – Нижний Новгород: ННГУ им. Н.И. Лобачевского. 2017. – 254с.

1.9. ИНФОРМАЦИОННОЕ И МЕДИАКОММУНИКАЦИОННОЕ ОБЕСПЕЧЕНИЕ ВОЕННОЙ ДЕЯТЕЛЬНОСТИ ОРГАНИЗАЦИИ СЕВЕРОАТЛАНТИЧЕСКОГО ДОГОВОРА НА СОВРЕМЕННОМ ЭТАПЕ

В исследовании раскрываются структурные аспекты универсума стратегических коммуникаций, определяющий информационное и медиакоммуникационное обеспечение военной деятельности вероятного противника России, а также нормативно-правовые и рекомендательные документы в сфере информационного и медиакоммуникационного обеспечения деятельности Североатлантического альянса, роли и полномочия ведущих должностных лиц и его органов, структура управления Североатлантического альянса, отвечающего за информационное и медиакоммуникационное обеспечение деятельности NATO в гражданской и военной сферах.
Ключевые слова: информационная безопасность, информационное и медиакоммуникационное обеспечение военной деятельности, Организация Североатлантического договора, NATO.

INFORMATION AND MEDIA COMMUNICATIONS SUPPORT OF MILITARY ACTIVITIES OF THE NORTH ATLANTIC TREATY ORGANIZATION AT THE PRESENT STAGE

The study reveals the structural aspects of the universe of strategic communications, which determines information and media communication support for the military activities of a potential enemy of Russia, as well as regulatory and advisory documents in the field of information and media communication support for the activities of the North Atlantic Alliance, the roles and powers of leading officials and its bodies, and the management structure The North Atlantic Alliance, responsible for information and media communications support for NATO activities in the civil and military spheres.
Key words: information security, information and media communication support for military activities, North Atlantic Treaty Organization, NATO.

Специальная военная операция на территории Украины (СВО) актуализировала в сфере современных военных действий информационный и медиакоммуникацонный уровень противоборства, который в Вооруженных Силах Российской Федерации нуждается в совершенствовании на уровне стратегических коммуникаций. Учитывая статус СВО как прокси-войны, в качестве объекта изучения опыта ведения информационных и психологических операций, реализуемых Центром информационно-психологических операций Вооруженных Сил Украины, (ЦИПсО ВСУ) мы определим органы информационного и медиакоммуникационного обеспечения военной деятельности Организации Североатлантического договора, их структуру, руководящие документы, принципы функционирования и т.п.

Современная Организация Североатлантического договора полагает, что разъяснение политики в области национальной обороны и безопасности, а также роли, которую играет та или иная страна в Североатлантическом альянсе, является прерогативой правительств отдельных государств-членов организации. Аналогично, каждая страна самостоятельно решает, какими методами информировать внутреннюю целевую аудиторию о политике и целях NATO, и какие ресурсы на это выделять. Все правительства государств-членов Организации Североатлантического договора признают демократическое право своих граждан на получение информации о международных структурах, обеспечивающих основу их безопасности, и важность

понимания и поддержки общественностью политики своей страны в сфере безопасности.

Непосредственная роль НАТО в области комплексного информационного и медиакоммуникационного обеспечения реализуемых действий, как в гражданской, так и военной сфере активности, состоит в том, чтобы дополнять деятельность по информированию общественности, ведущуюся в каждом государстве-участнике, за счет разъяснения политики и целей Организации Североатлантического договора, привлечения широкой общественности к конструктивному и основанному на фактах обсуждению актуальных проблем, организации программ, предназначенных для общественных деятелей, журналистов, ученых, парламентских групп, молодежи и работников образования, а также стимулирования непрерывных дискуссий и разработки политики по вопросам международной безопасности.

Указанная разъяснительная и информационная, а в целом – пропагандистская деятельность – реализуется по направлениям «публичная дипломатия» и «связи с общественностью (в гражданской и военной сферах)» в рамках коммуникативной системы Североатлантического альянса, получившей наименование «стратегические коммуникации», в состав которой, помимо указанных, входят такие направления, как «информационные операции» и «психологические операции» (См. Рис. 1).

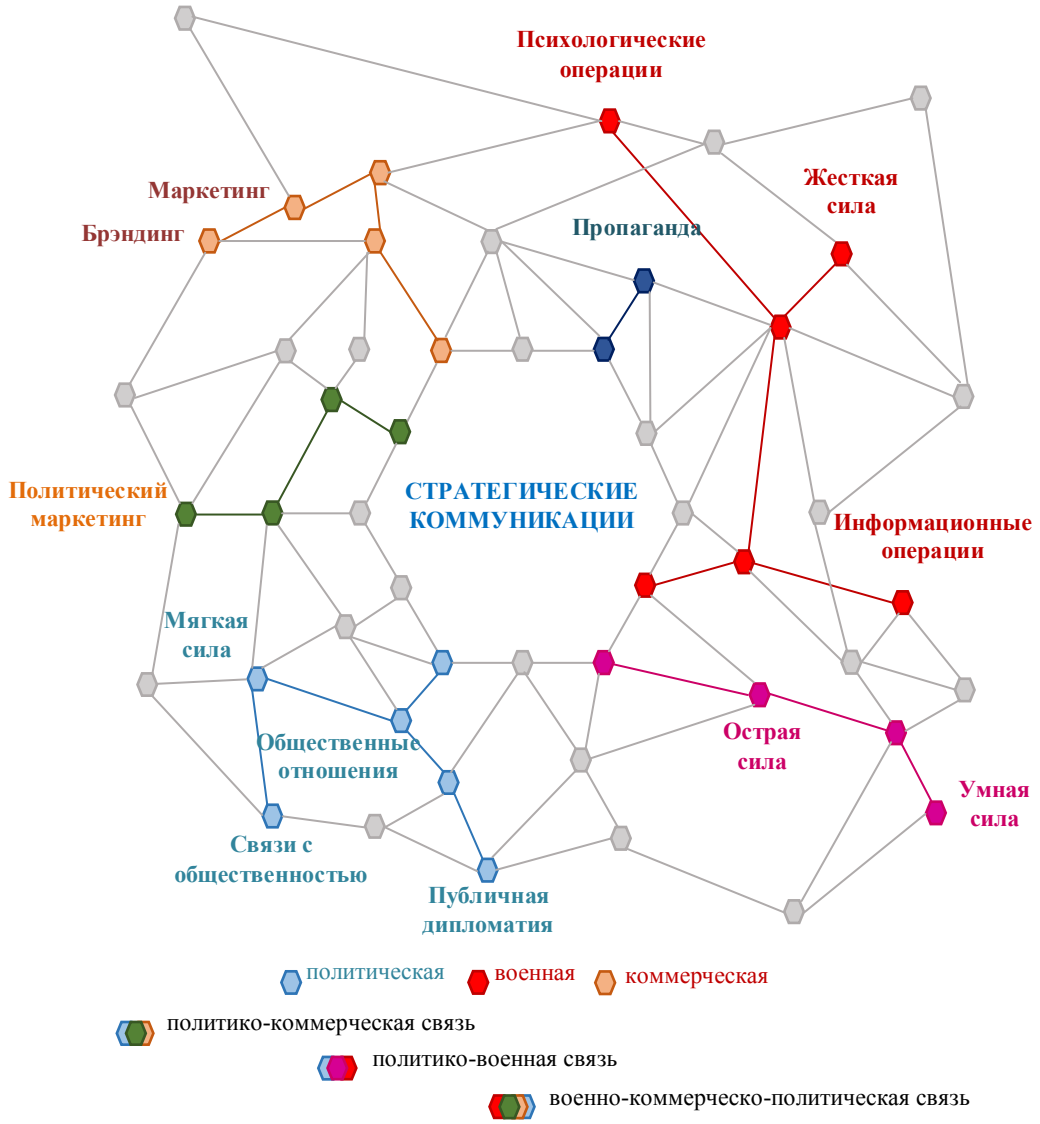


Рисунок 1 - Универсум стратегических коммуникаций

В современной терминологии Североатлантического альянса, согласно публикации Центра передового опыта Организации Североатлантического договора в сфере стратегических коммуникаций (англ. *NATO Strategic Communications Centre of Excellence, NATO StratCom CoE*) от июня 2019 г. «Совершенствование терминологии Организации Североатлантического договора в сфере стратегических коммуникаций» (англ. *Improving NATO Strategic Communications Terminology*), названные выше система и направления, представленные как универсум на рисунке 1, трактуются следующим образом:

1) ***стратегические коммуникации*** (англ. *Strategic Communications, StratCom*) – это скоординированное и надлежащее использование коммуникационных действий и возможностей (сил и средств) Североатлантического альянса – публичной дипломатии, связей с общественностью в гражданской и военной сферах, информационных и психологических операций (в зависимости от обстоятельств) – в поддержку политики, операций и мероприятий альянса, а также для достижения целей Организации Североатлантического договора;

2) ***публичная дипломатия*** (англ. *Public Diplomacy*) – это коммуникационные и информационно-пропагандистские меры и инструменты, реализуемые и применяемые Организацией Североатлантического договора в гражданской сфере в дополнение к национальным усилиям союзников, предназначенные для повышения осведомленности, углубления понимания и поддержки политики, операций и действий Североатлантического альянса в краткосрочной, среднесрочной и долгосрочной перспективе;

3) ***связи с общественностью в гражданской сфере (гражданские связи с общественностью)*** (англ. *Public Affairs (civilian)*) – это обязательство Организации Североатлантического договора в гражданской сфере, предусматривающее своевременное, точное, оперативное и заблаговременное (проактивное) информирование общественности через средства массовой информации (коммуникации) относительно политики, операций и действий Североатлантического альянса;

4) ***связи с общественностью в военной сфере (военные связи с общественностью)*** (англ. *Military Public Affairs*) – это функция, ответственная за продвижение военных целей и задач Организации Североатлантического договора среди аудиторий в интересах повышения осведомленности и понимания военных аспектов Североатлантического альянса. Она включает в себя планирование и осуществление сношений со средствами массовой информации (коммуникации), внутренних коммуникаций и поддержание отношений с местным сообществом. Военные связи с общественностью на каждом уровне командования призваны оказывать непосредственную поддержку командующему и поэтому не могут быть дополнительно делегированы или вменены персоналу, исполняющему другие функции;

5) ***информационные операции*** (англ. *Information Operations, InfoOps*) – это военная функция, обеспечивающая предоставление рекомендаций и координацию военно-информационных действий, одобренных Советом Североатлантического договора (Североатлантическим советом) (англ. *North Atlantic Council, NAC*), с целью создания желаемого воздействия на волю, понимание и способности противников, потенциальных противников и других сторон в интересах поддержки операций, миссий и целей Североатлантического альянса;

6) ***психологические операции*** (англ. *Psychological Operations, PSYOPS or PsyOps*) – это заблаговременно планируемые психологические мероприятия, ориентированные на утвержденные аудитории и реализуемые в интересах влияния на их восприятие, отношение и поведение за счет использования методов коммуникации и других средств, оказывающие существенное воздействие на достижение политических и военных целей.

Соотношение основных компонентов стратегических коммуникаций представлено в таблице 1.

Таблица 1 – Соотношение основных компонентов стратегических коммуникаций

Показатели	**Информационные операции**	**Психологические операции**	**Публичная дипломатия**	**Связи с общественностью**
Наличие специализированных органов управления	Проводятся под руководством органов управления военными операциями	Отделы/отделения психологических операций	Органы управления по вопросам публичной дипломатии	Отделы/отделения связей с общественностью
Цели деятельности	Достижение информационного превосходства над противником в интересах реализации политики NATO и успешного проведения операций альянса			
Общая направленность деятельности	Формирование благоприятной для NATO информационной среды	Воздействие на сознание и деятельность целевых аудиторий	Формирование общественного мнения в поддержку политики и операций NATO	Информирование населения о целях деятельности и решаемых NATO задачах
Целевые аудитории	Общество в целом (руководящие органы, гражданское население и военнослужащие, общественные институты) своих, дружественных и враждебных стран	Информационные источники, органы управления различных уровней, население и силовые структуры противника	Руководство государств-членов NATO и стран-партнеров, международные и неправительственные организации	Местные органы власти, население вовлеченных в конфликты стран, их средства массовой информации (коммуникации) (СМИ(К))
Полномочия по работе с информацией	Добывание, обработка и распространение текущей информации	Обработка и распространение специальной информации	Распространение предоставленной информации	Распространение предоставленной информации
Категории информационных материалов	Заслуживающие доверия и обработанные сообщения	Отобранная и надлежащим образом интерпретированная специальная информация	Вся разрешенная информация	Вся разрешенная информация
Результаты деятельности	Достижение свободы действий в информационном пространстве, обеспечение защиты своей информации и подавление информационных структур противника	Принятие желаемых решений и достижение необходимого поведения целевых аудиторий	Установление устойчивого взаимодействия и взаимопонимания со всеми участниками урегулирования кризисных ситуаций	Повышение доверия к NATO, подтверждаемое опросами общественного мнения

На сегодняшний день деятельность НАТО в сфере информационного и медиакоммуникационного обеспечения проводимых гражданских и военных мероприятий регламентируется рядом нормативно-правовых документов и документов, носящих рекомендательный характер, перечень которых представлен в таблице 2.

Таблица 2 – Нормативно-правовые и рекомендательные документы в сфере информационного и медиакоммуникационного обеспечения деятельности НАТО

Тип документа	**Наименование документа**	**Дата публикации**	**Сущность**
Политика	Политика Организации	29 сентября	

Тип документа	Наименование документа	Дата публикации	Сущность
(программный документ) *(англ. Policy)*	Североатлантического договора в области стратегических коммуникаций (англ. *PO (2009)0141 NATO Strategic Communications Policy*)	2009 г.	
	Военная политика Организации Североатлантического договора в области стратегических коммуникаций (англ. *MC 0628 NATO Military Policy on Strategic Communications*)	10 июля 2017 г.	
	Военная политика Организации Североатлантического договора в области психологических операций (англ. *Policy MC 0402/2 NATO Military Policy on Psychological Operations*)	03 октября 2012 г.	Психологические операции – это коммуникационные возможности, координируемые с информационными операциями исходя из структуры стратегических коммуникаций НАТО
	Военная политика Организации Североатлантического договора по вопросам гражданского и военного сотрудничества и военно-гражданского взаимодействия (англ. *MC 0411/2 NATO Military Policy on Civil-Military Cooperation (CIMIC) and Civil-Military Interaction (CMI)*)	12 мая 2014 г.	Взаимодействие между гражданскими и военными органами и структурами разъясняется военно-политическим руководством в сфере стратегических коммуникаций для синхронизации обмена сообщениями и операций
	Военная политика Организации Североатлантического договора в области информационных операций (англ. *MC 0422/5 NATO Military Policy for Information Operations)*	11 сентября 2018 г.	Информационные операции – это штабная функция, координирующая все возможности Объединенного оперативного штаба, исходя из структуры стратегических коммуникаций НАТО
	Военная политика Организации Североатлантического договора в области связей с общественностью (англ. *MC 0457/2 NATO Military Policy on Public Affairs*)	08 февраля 2011 г.	Связи с общественностью – это коммуникационный потенциал, координируемый исходя из структуры стратегических коммуникаций НАТО
Совместная союзническая публикация 1 уровня *(англ. Allied Joint Publication (AJP, Level 1))*	Совместная союзническая публикация № 01(D) «Совместная доктрина союзников» *(англ. AJP-01(D) Allied Joint Doctrine)*	декабрь 2010 г.	Базовый документ
	Совместная союзническая публикация № 3(C) «Совместная доктрина союзников для проведения операций» *(англ. AJP-3(C) Allied Joint Doctrine for the Conduct of Operations)*	издание C (пересмотренное), версия 1	Стратегические коммуникации включены в перечень подлежащих рассмотрению проблем оперативного уровня для совместных и многонациональных операций
	Совместная союзническая публикация № 5 «Совместная доктрина союзников для планирования оперативного	июнь 2013 г.	Стратегические коммуникации включены в перечень ведущих принципов для

Тип документа	Наименование документа	Дата публикации	Сущность
	уровня» *(англ. AJP-5 Allied Joint Doctrine for Operational-level Planning)*		союзнических совместных и многонациональных операций
Совместная союзническая публикация 2 уровня *(англ. Allied Joint Publication (AJP, Level 2))*	Совместная союзническая публикация № 3.10 «Совместная доктрина союзников в области информационных операций» *(англ. AJP-3.10 Allied Joint Doctrine for Information Operations)* [1]	издание А, версия 1 (декабрь 2015 г.)	Данная доктрина согласуется с соответствующей ей политикой
	Совместная союзническая публикация № 3.10.1 «Совместная доктрина союзников в области психологических операций» *(англ. AJP-3.10.1 Allied Joint Doctrine for Psychological Operations)* [2]	издание В, версия 1 (сентябрь 2014 г.)	Данная доктрина служит основой, помогающей командующим и их подчиненным думать, планировать и действовать. Она сосредоточена на оперативном уровне, но также имеет практическую ценность для стратегического и тактического уровней
	Совместная союзническая публикация № 3.2 «Совместная доктрина союзников в области наземных операций» *(англ. AJP-3.2 Allied Joint Doctrine for land operations)* [3]	издание А, версия 1 (март 2016 г.)	Большинство операций осуществляется на суше
	Совместная союзническая публикация № 3.4(A) «Совместная доктрина союзников в области операций по реагированию на кризисы, не предусмотренных статьей 5» *(англ. AJP-3.4(A) Allied Joint Doctrine for Non-article 5 Crisis Response Operations)*	все еще не утверждена	Один из наиболее важных видов операций НАТО
Союзническая административная публикация *(англ. Allied Administrative Publication*	Союзническая административная публикация № 06 «Глоссарий терминов и определений Организации Североатлантического договора» *(англ. AAP 06 NATO Glossary of Terms and Definitions)*	редакция от 11 ноября 2019 г.	Собранные термины и определения являются утвержденными и используются всеми государствами-участниками НАТО
Руководство *(англ. Handbook)*	Руководство Организации Североатлантического договора по стратегическим коммуникациям, версия 1.0 *(англ. NATO Strategic Communications Handbook, Version 1.0)* [4]	21 сентября 2017 г.	Руководство применяется командованиями НАТО всех уровней и их штаб-квартирами
	Военная стратегическая коммуникация в коалиционных операциях – руководство для использования на практике, версия 0.2 *(англ. Military Strategic Communication in Coalition Operations - A Practitioners Handbook (MilStratCom Handbook), Version 0.2)* [5]	21 октября 2016 г.	Руководство применяется командованиями НАТО всех уровней и их штаб-квартирами, командованиями коалиционных войск и их штаб-квартирами при проведении операций
	Руководство по связям с общественностью, изданное под	версия мая	Руководство применяется командованиями ГАТО всех

Тип документа	Наименование документа	Дата публикации	Сущность
	эгидой Объединенного командования операциями и Объединенного командования по трансформации НАТО (англ. *Allied Command Operations and Allied Command Transformation Public Affairs Handbook*) [6]	2020 г.	уровней и их штаб-квартирами

Роли и полномочия ведущих должностных лиц и органов Североатлантического альянса в сфере информационного и медиакоммуникационного обеспечения гражданской и военной деятельности раскрыты в таблице 3. Их специфическая иерархическая структура показана на рисунке 2.

Таблица 3 – Роли и полномочия ведущих должностных лиц и органов НАТО в сфере информационного и медиакоммуникационного обеспечения гражданской и военной деятельности

Юридическое лицо	Роль (назначение)
Совет Североатлантического договора (Североатлантический совет) (англ. *North Atlantic Council, NAC*)	Обеспечивает общее руководство и управление деятельностью Североатлантического альянса в сфере стратегических коммуникаций, а также стратегическое и политическое руководство информационными мероприятиями НАТО в рамках конкретных миссий
Генеральный секретарь (англ. *Secretary General, SG*)	Обеспечивает руководство и управление стратегическими коммуникациями в рамках своего предназначения. Является главным официальным представителем (спикером, пресс-секретарем) НАТО на всех уровнях
Официальный представитель (пресс-секретарь, спикер) Организации Североатлантического договора (англ. *NATO Spokesperson*)	От имени Генерального секретаря обеспечивает ежедневное управление всеми действиями штаб-квартиры Организации Североатлантического договора в сфере взаимодействия со средствами массовой информации (коммуникации), включая передачу и обмен сообщениями. Разрабатывает указания и предложения относительно руководства связями с общественностью в военной сфере для обеспечения того, чтобы все сообщения и коммуникации НАТО соответствовали избранному политическому направлению и принятым на политическом уровне решениям
Помощник Генерального секретаря по вопросам публичной дипломатии – начальник отдела публичной дипломатии (англ. *Assistant Secretary General for Public Diplomacy, ASG PDD*)	Осуществляет контроль над координацией всех действий, реализуемых в рамках стратегических коммуникаций, во всех гражданских и военных органах, а также командованиях Североатлантического альянса. Осуществляет руководство всеми мероприятиями, организуемыми в области публичной дипломатии под эгидой штаб-квартиры НАТО
Военный комитет (англ. *Military Committee, MC*)	Обеспечивает общую политику Организации Североатлантического договора для связей с общественностью в военной сфере, информационных и психологических операций, а также консультирует Североатлантический совет по военным аспектам стратегических коммуникаций
Председатель Военного комитета (англ. *Chairman of the Military Committee, CMC*)	Является главным официальным военным представителем (спикером, пресс-секретарем) НАТО
Офис советника по связям с общественностью и стратегическим коммуникациям Международного военного штаба (англ. *International Military Staff (IMS)*	Обеспечивает освещение деятельности Военного комитета, его председателя и руководителя Международного военного штаба по вопросам стратегических коммуникаций. Предоставляет рекомендации генеральному директору и

Юридическое лицо	Роль (назначение)
Office of the Public Affairs and StratCom Advisor (PASCAD), IMS PASCAD)	руководителям подразделений Международного военного штаба по всем вопросам связей с общественностью, устанавливает и поддерживает связь с подразделениями публичной дипломатии и связей с общественностью штаб-квартиры Верховного главнокомандующего Объединенными вооруженными силами НАТО в Европе, Верховного главнокомандующего по трансформации Объединенных вооруженных сил Организации Североатлантического договора и всех объединенных командований, национальными делегациями Организации Североатлантического договора и национальными департаментами связей с общественностью в объединенных службах начальников штабов и министерствах обороны. Является главным контактным центром по вопросам стратегических коммуникаций в составе Международного военного штаба
Отдел информационных операций Международного военного штаба (англ. *International Military Staff (IMS) Information Operations (InfoOps), IMS InfoOps*)	Отвечает за политику Военного комитета в отношении информационных и психологических операций, содействует сотрудничеству между двумя стратегическими командованиями и Военным комитетом по вопросам информационных и психологических операций
Верховный главнокомандующий Объединенными вооруженными силами Организации Североатлантического договора в Европе (англ. *Supreme Allied Commander Europe, SACEUR*)	Предоставляет руководящие указания в области стратегических коммуникаций, осуществляемых в рамках Объединенного командования операциями (англ. *Allied Command Operations, ACO*), включая такие направления, как связи с общественностью в военной сфере, информационные и психологические операции, в соответствии с общими указаниями в области стратегических коммуникаций, исходящими из штаб-квартиры НАТО (Североатлантического совета, Генерального секретаря и Военного комитета Североатлантического альянса). Является главным официальным военным представителем (спикером, пресс-секретарем) по текущим операциям НАТО
Верховный главнокомандующий по трансформации Объединенных вооруженных сил Организации Североатлантического договора (англ. *Supreme Allied Commander Transformation, SACT*)	Обеспечивает руководство стратегическими коммуникациями в рамках Объединенного командования по трансформации (англ. *Allied Command Transformations, ACT*), развитие концепции и возможностей стратегических коммуникаций в тесном взаимодействии с Объединенным командованием операциями. Является главным официальным военным представителем (спикером, пресс-секретарем) по вопросам трансформации Объединенных вооруженных сил НАТО
Руководитель стратегическими коммуникациями штаб-квартиры Верховного главнокомандующего Объединенными вооруженными Силами Организации Североатлантического договора в Европе (руководитель отдела внешних сношений (коммуникаций)) (англ. *Supreme Headquarters Allied Powers Europe (SHAPE) Chief StratCom / Director of Communications*)	Отвечает перед Верховным главнокомандующим Объединенными вооруженными силами Североатлантического альянса в Европе за разработку и интеграцию планов стратегических коммуникаций в поддержку текущих операций НАТО и действий Объединенного командования операциями в соответствии с общим указанием относительно стратегических коммуникаций, исходящим из штаб-квартиры НАТО; координирует мероприятия по связям с общественностью в военной сфере, информационные и психологические операции, реализуемые для поддержки планов стратегических коммуникаций; осуществляет контроль над выполнением планов стратегических коммуникаций во взаимодействии со

Юридическое лицо	Роль (назначение)
	штаб-квартирой НАТО и штаб-квартирами, подчиненными Объединенному командованию операциями
Старший офицер (главный сотрудник) по связям с общественностью штаб-квартиры Верховного главнокомандующего Объединенными вооруженными Силами Организации Североатлантического договора в Европе (англ. *SHAPE Chief Public Affairs Officer, SHAPE PAO*)	Направляет, планирует и осуществляет связи с общественностью в военной сфере для поддержки текущих операций Организации Североатлантического договора и действий Объединенного командования операциями на стратегическом уровне
Старший офицер (главный сотрудник) по связям с общественностью Верховного главнокомандующего по трансформации Объединенных вооруженных сил Организации Североатлантического договора (англ. *SACT Chief Public Affairs Officer (PAO), SACT PAO*)	Направляет, планирует и осуществляет связи с общественностью в военной сфере для поддержки действий Объединенного командования НАТО по трансформации (англ. *Allied Command Transformations, ACT*) на стратегическом уровне

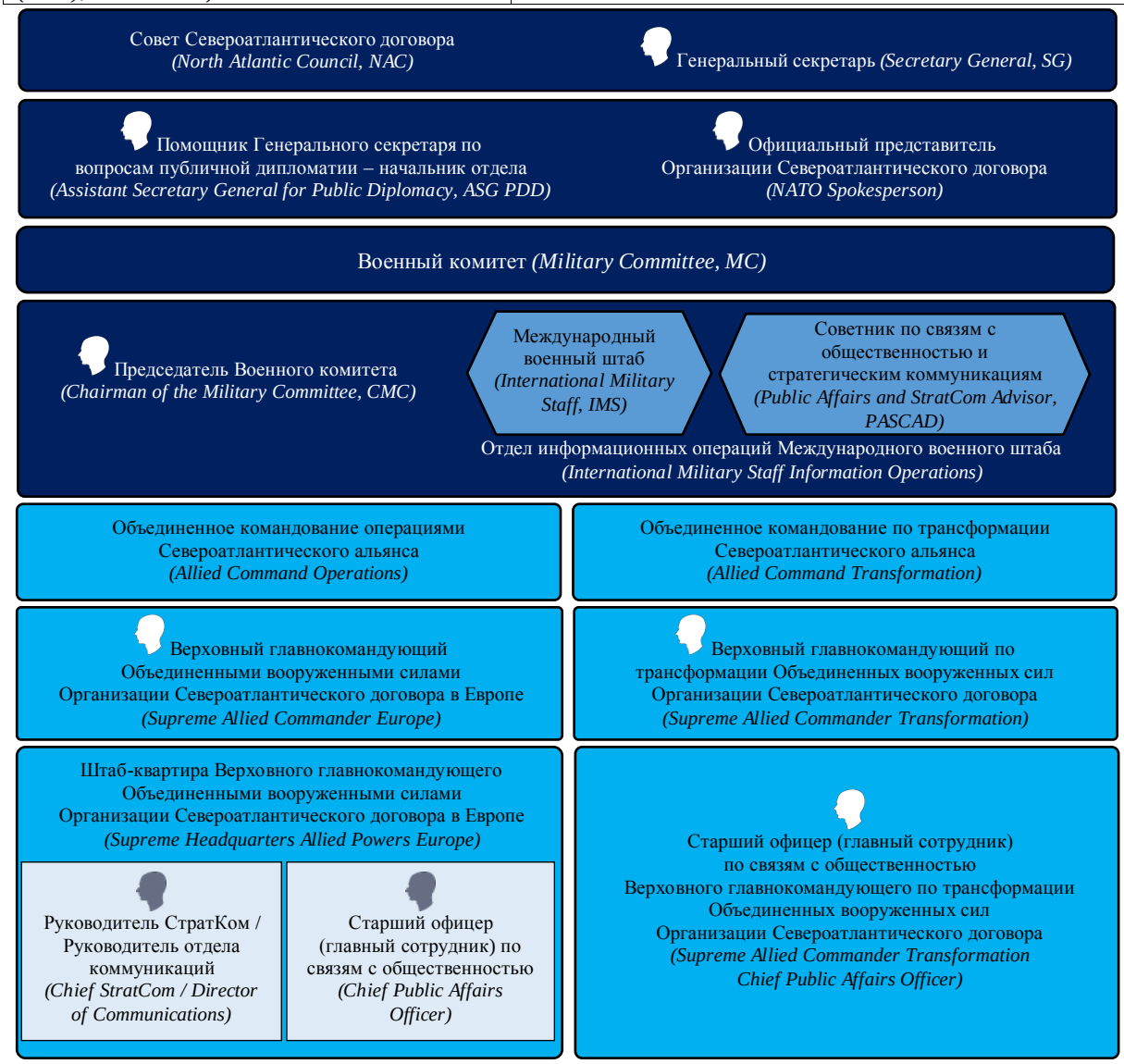


Рисунок 2 – Элементы структуры управления Североатлантического альянса, отвечающие за информационное и медиакоммуникационное обеспечение деятельности NATO в гражданской и военной сферах

Учитывая сложность и неоднозначность проблемы стратегических коммуникаций, в январе 2014 г. правительством Латвии было принято решение о создании Центра передового опыта НАТО. Его соучредителями стали Литва, Эстония, Соединенное королевство Великобритании и Северной Ирландии, Италия, Германия и Польша. Соединенные Штаты Америки от участия в проекте отказались. В сентябре этого же года Центр передового опыта в сфере стратегических коммуникаций (электронный адрес: *www.stratcomcoe.org*; e-mail: *info@stratcomcoe.org*) прошел процедуру аккредитации, а с 20 августа 2015 г. был размещен в новом охраняемом здании недалеко от центра Риги.

По словам директора Центра передового опыта Организации Североатлантического договора в сфере стратегических коммуникаций Яниса Сартса, подчиняющегося Координационному комитету, состоящему из представителей стран-спонсоров и возглавляемому сотрудником Министерства обороны Латвии (См. Рис. 3), в учреждении работают 33 военных и гражданских специалиста из 12 европейских стран и Канады. Должность заместителя директора центра занимает полковник Вооруженных сил Эстонии Пеэтер Тали, а должность менеджера по связям с общественностью – Линда Цурика.

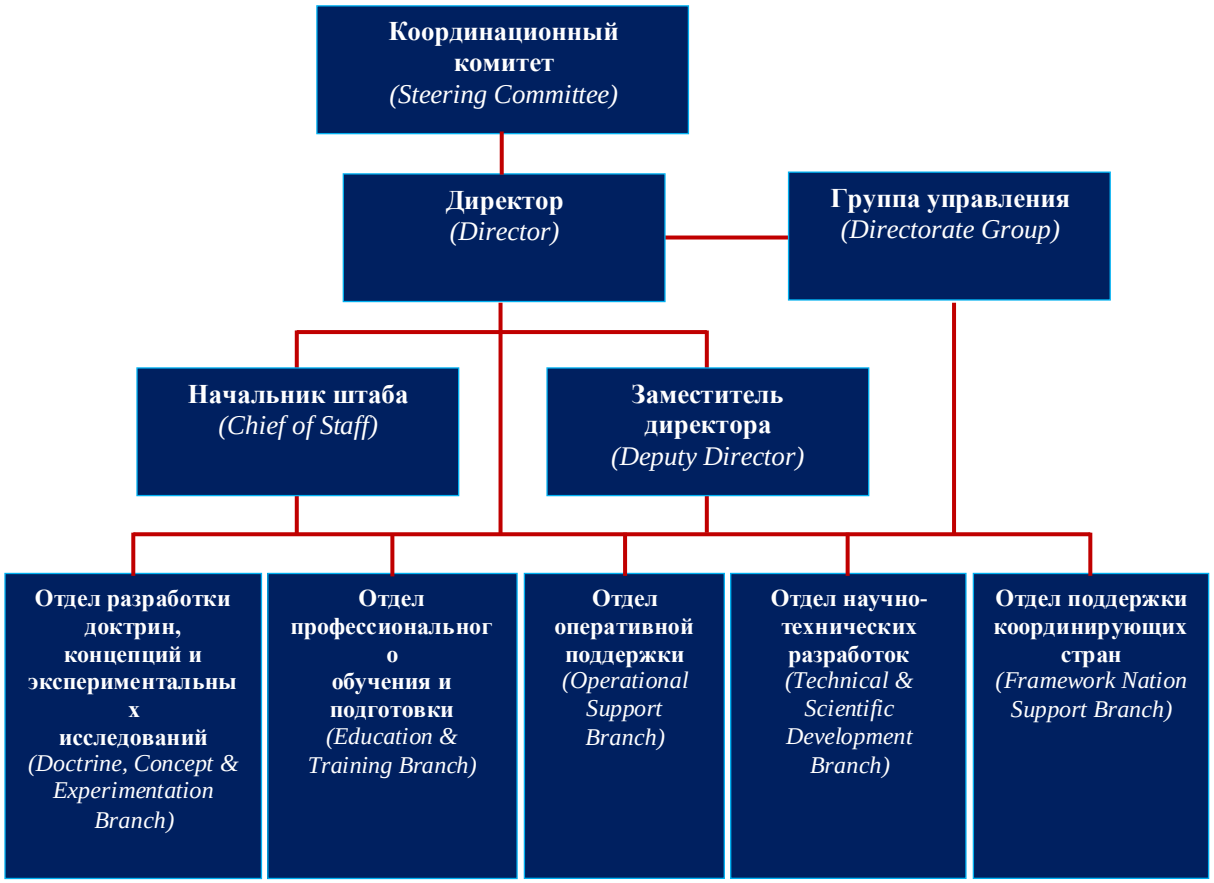


Рисунок 3. - Структура Центра передового опыта НАТО в сфере стратегических коммуникаций

По мнению П. Тали [7], создание Центра, в первую очередь, стало ответом европейских стран на режим В.В. Путина, который «не терпит кооперации, консенсуса и ценностного подхода»: «Кремль использует модель DIME, то есть «Diplomacy», «Information», «Military», «Economic» [в пер. с англ. – дипломатия, информация, военная сила, экономика]. Ее цель – находить «трещины» в структурах и явлениях, которые он считает враждебными, и увеличивать эти «трещины» до больших «разломов», «расколов». Поиск таких «трещин» идет на всех уровнях: стратегическом,

оперативном и тактическом. Стратегический уровень – это международные организации, начиная с ООН, ЕС, NATO. В оперативном плане – это поиск «трещин» на уровне отдельных государств и межгосударственных отношений. Например, между Эстонией и Латвией, Эстонией и Финляндией, между Украиной и Польшей, Украиной и Венгрией. Какую-то «трещинку» практически всегда можно найти. … Прежде всего, Кремль дискредитирует само понятие «свобода слова». Он старается сеять информационный туман, распространяя установку, что не нужно верить журналистам. Посмотрите, например, на слоган каналов «Sputnik» и «Russia Today»: «Telling the Untold» [«Говорим о том, о чем другие молчат»]. Не скажу, что это нечто совершенно уж новое. Когда-то чем-то подобным занималось Агентство печати «Новости» [созданное в 1961 г. на базе «Совинформбюро» для внешнеполитической пропаганды, в 1991 г. преобразованное в РИА «Новости», а в декабре 2013 г. – в МИА «Россия сегодня»]. Однако цифровизация создала новые возможности для деятельности этих структур и сегодня «Sputnik» и «Russia Today» доступны всем. При этом со стопроцентной уверенностью можно утверждать, что обе структуры не являются медиа и журналистикой не занимаются. Тут лучше подходит определение, данное как-то Сергеем Шойгу: в наше время медиа – это просто система оружия…» [8].

Главными целями Центра передового опыта в сфере стратегических коммуникаций являются обмен опытом и координация деятельности структур Североатлантического альянса и стран-партнеров, занимающихся публичной дипломатией и связями с общественностью, проведением информационных и психологических операций. Кроме того, данный Центр осуществляет подготовку специалистов в области стратегических коммуникаций, проводит различного рода научно-исследовательские работы по обобщению опыта информационных кампаний и выработке новых форм и методов влияния на целевые аудитории. Он функционирует в тесном сотрудничестве с расположенным в Таллине эстонским Объединенным центром передового опыта Организации Североатлантического договора в сфере кибернетической защиты (англ. *NATO Cooperative Cyber Defence Centre of Excellence, NATO CCD CoE*).

Работа Центра осуществляется на основе следующих принципов:

- в деятельности Центра могут принимать участие все государства-члены Организации Североатлантического договора, для них открыт полный доступ к его продукции и услугам;
- дублирование функций других органов Североатлантического альянса исключается;
- функционирование Центра осуществляется в соответствии с меморандумом о взаимопонимании, который может дополняться по мере необходимости;
- в своей деятельности Центр использует существующие и новые информационные технологии, которые содействуют достижению успеха Организации Североатлантического договора в виртуальной среде;
- организация Центра и взаимодействие между его структурными элементами осуществляются в соответствии с руководящими документами;
- Латвия, в лице Министерства обороны, предоставляет необходимые для работы Центра инфраструктуру и оборудование;
- рабочий язык Центра – английский.

Доктрина развития Центра предполагает:

- поддержку политики НАТО, а также формирование концепций, которые содействуют развитию потенциала в области стратегических коммуникаций, как в рамках альянса, так и в отдельных государствах-членах;
- содействие национальным и многонациональным усилиям по разработке концепций, публикаций, стандартов, процедур и терминологии в сфере стратегических коммуникаций;

- адаптацию и обновление существующей политики, доктрин и концепций в сфере стратегических коммуникаций в соответствии с изменениями военно-политической обстановки;

- подготовку и внедрение в процесс планирования военных операций НАТО вопросов, касающихся стратегических коммуникаций;

- разработку предложений по оптимизации деятельности в сфере стратегических коммуникаций и обеспечение реализации решений, принятых в данной области;

- оказание поддержки штаб-квартирам НАТО по формированию руководящих принципов в сфере стратегических коммуникаций.

К числу основных задач Центра относятся:

- изучение и анализ информационной среды, определение тематики и форм воздействия на утвержденные Североатлантическим советом целевые аудитории;

- формирование в странах, входящих в зону интересов НАТО, радикальной оппозиции из числа подверженных манипулированию групп населения; организация связей с общественностью в интересах формирования позитивного отношения к политике Североатлантического альянса;

- консультирование руководства НАТО и стран-партнеров по вопросам современных тенденций развития информационного пространства;

- содействие исследованиям, проводимым в области использования технологий информационного воздействия в военных целях;

- разработка средств и методов противодействия информационно-пропагандистской деятельности специализированных структур государств, не входящих в состав НАТО;

- разработка специализированных научно-образовательных программ по популяризации деятельности Североатлантического альянса;

- предоставление заинтересованным органам Североатлантического альянса технических и специальных знаний в области стратегических коммуникаций, призванных способствовать более качественному проведению информационных и психологических операций;

- обеспечение коалиционных органов Североатлантического альянса оперативной информацией, связанной с вопросами стратегических коммуникаций, а также выявление тенденций в данной сфере;

- осуществление оперативного планирования стратегических коммуникаций;

- определение потенциальных потребностей и возможностей Североатлантического альянса в области стратегических коммуникаций;

- анализ и оценка результатов взаимодействия со СМИ(К) и общественными организациями, а также информационной работы в ходе оперативной деятельности Североатлантического альянса;

- развитие альтернативных источников передачи информации, а также изучение их влияния на общественное сознание (культура, слухи, идеология и религия);

- анализ действующих или планирование новых операций в сфере стратегических коммуникаций в интересах реагирования на изменение обстановки в разыгрываемых сценариях;

- использование разработок из других областей науки (лингвистики, антропологии, менеджмента, теории коммуникаций и психологии) в интересах стратегических коммуникаций;

- поиск и анализ идей, концепций и технологий частных компаний, промышленности и исследовательских центров с целью их интегрирования в стратегию деятельности НАТО.

Кроме того, в функции Центра входит:

- оказание помощи в разработке, проверке и доведении руководящих принципов стратегических коммуникаций до стран-партнеров;

- организация взаимодействия с другими центрами НАТО и продвижение собственных курсов и программ;

- распространение передового опыта в ходе планирования и проведения информационных кампаний;

- оказание помощи структурам НАТО в рамках проведения мероприятий, касающихся стратегических коммуникаций, и активизация практических действий на всех уровнях;

- проведение конференций, семинаров, практикумов и информационных кампаний с целью выработки политики НАТО в области стратегических коммуникаций; обеспечение подготовки оперативных групп для специальных операций Североатлантического альянса;

- разработка пособий и справочников в рамках компетенции Центра;

- организация виртуальной рабочей среды для привлечения международных экспертов, а также повышение ее гибкости и доступности в зависимости от развития ситуации; ведение Интернет-сайта, позволяющего осуществлять взаимодействие между экспертами в сфере стратегических коммуникаций с помощью электронной почты, социальных сетей, блогов, справочников, веб-приложений и сайтов обмена видеоинформацией;

- оказание содействия руководству НАТО в организации мультимедийных конференций и конференций в социальных сетях;

выступление в качестве посредника между НАТО, другими странами и заинтересованными сторонами (промышленность, научные круги, неправительственные организации) по вопросам, касающимся стратегических коммуникаций.

Таким образом, ретроспективное изучение правовых и организационных основ информационного и медиакоммуникационного обеспечения военной деятельности НАТО, с одной стороны, свидетельствует о фундаментальном подходе последнего к реализации своих военных целей, а, с другой стороны – должен инициировать работу по созданию структур в армии России, способных ей противостоять. Военно-политическое руководство должно учитывать возможности НАТО по тотальному переформатированию общественного сознания целых стран (Украина, Молдова и т.п.), использовать их опыт в контрборьбе, искать уязвимости и формировать направления противодействия информационным и психологическим операциям коллективного запада против России.

Перечень используемой литературы и источников:

1. AJP-3.10 Allied Joint Doctrine for Information Operations. – URL: https://info.publicintelligence.net/NATO-IO.pdf (дата обращения: 15.11.2023).
2. AJP-3.10.1 Allied Joint Doctrine for Psychological Operations. – URL: https://info.publicintelligence.net/NATO-PSYOPS.pdf (дата обращения: 15.11.2023).
3. AJP-3.2 Allied Joint Doctrine for land operations. – URL: https://www.coemed.org/files/stanags/01_AJP/AJP-3.2_EDA_V1_E_2288.pdf (дата обращения: 15.11.2023).
4. NATO Strategic Communications Handbook, Version 1.0. – URL: https://d3n8a8pro7vhmx.cloudfront.net/lymec/pages/875/attachments/original/-NATO-STRATEGIC-COMMUNICATIONS-HANDBOOK-DRAFT-FOR-USE-2015-BI.pdf? (дата обращения: 15.11.2023).
5. Military Strategic Communication in Coalition Operations – A Practitioners Handbook. – URL: https://info.publicintelligence.net/MCDC-MilStratComHandbook.pdf (дата обращения: 15.11.2023).
6. Allied Command Operations and Allied Command Transformation Public Affairs Handbook. – URL: https://www.act.nato.int/wp-content/uploads/2023/06/nato-pao-handbook-2020.pdf (дата обращения: 15.11.2023).
7. Тали Пеэтер. – URL: https://geochronic.ru/index.php?title (дата обращения: 14.11.2023).
8. Тали П. Российская пропаганда – в НАТО рассказали, как это работает. – URL: https://politics.segodnya.ua/politics/v-nato-rasskazali-kak-rossiya-raskalyvaet-edinstvo-zapada-1360966.html (дата обращения: 14.11.2023).

1.10. МЕТОДИКИ РАЗРАБОТКИ ЗАЩИТЫ ИНФОРМАЦИОННЫХ СИСТЕМ ОТ DDOS-АТАК НА ОСНОВЕ ПРИМЕНЕНИЯ АЛГОРИТМОВ РОЕВОГО ИНТЕЛЛЕКТА

Представленная автором работа посвящена разработке методики защиты информационных систем на основе алгоритмов роевого интеллекта от Ddos-атак. В статье предложена методика обучения нейронной сети с использованием метода роя частиц и рассмотрена модель разрабатываемой сети с процессом её обучения. Представлены результат работы, представляющий собой программный комплекс обучения и тестирования создаваемой сети, и анализ предлагаемого метода защиты информации на точность и эффективность распознавания вредоносных атак.
Ключевые слова: информационные технологии (ИТ), искусственный интеллект (ИИ), защита от Ddos-атак, метод роя частиц, нейронные сети (НС).

METHODS FOR DEVELOPING INFORMATION SYSTEMS PROTECTION FROM DDOS ATTACKS BASED ON THE APPLICATION OF SWARM INTELLIGENCE ALGORITHMS

The work presented by the author is devoted to the development of a method for protecting information systems based on swarm intelligence algorithms from Ddos attacks. The article proposes a method for training a neural network using the particle swarm method and considers the model of the developed network with the process of its training. The result of the work is presented, which is a software package for training and testing the created network, and an analysis of the proposed method of information protection for the accuracy and efficiency of recognizing malicious attacks.
Keywords: information technology (IT), artificial intelligence (AI), protection against DDoS attacks, particle swarm method, neural networks (NS).

Введение. В настоящий момент благодаря углубленной познавательной деятельности, человечество достигло больших успехов в сфере информационных технологий (ИТ), создали глобальную сети, компактные методы хранения информации доступной всем пользователям, так же значимым новшеством стало создание нейронных сетей (НС). Свободный доступ к обширным данным должен сопровождаться защитой от внешнего вмешательства в целостность информации. Однако с развитием нейронных сетей они нашли применение во всей области ИТ, так же в области защиты информации.

Преимущество НС заключается в том, что при должном обучении и настройке, она позволяет выполнять трудоемкую работу за считаные мгновения, тем самым эффективно предотвращает непредвиденные ситуации, например, падение производительности сервера, ошибок на стороне сервера или же внешних вредоносных атак.

Постановка задачи. Цель разрабатываемого проекта основана на создании программного модуля защиты информации от Ddos-атак с применением НС, обученных на алгоритмах роевого интеллекта. Цель разрабатываемого модуля, основанный на методике защиты информации с помощью НС, сохранить целостность и конфиденциальности данных от Ddos-атак путем анализа входящего трафика, определяя тип данного трафика безопасный он или нет, предоставляя соответственно доступ к данным или же блокировку входящих пакетов данных.

Разработка методики. Для оптимизации параметров создаваемой НС был применён алгоритм роя частиц предложенным в 1998 году американскими исследователями в области математики и информатики Юхи Ши и Расселом С. Эберхартом [4] и дополнительно модифицирован под наши задачи. В частности, веса синапсов во время обучения корректируются методом обратного распространения стандартной ошибки, а также корректируются методом роя частиц. Однако такой корректор, как метод роя частиц, следует использовать только в том случае, если

результат работы нейронной сети с высокой точностью соответствует ожидаемым результатам, иначе использование данного алгоритма значительно меняет веса синапсов, тем самым создавая дополнительную погрешность результата [2].

Модель нейронной сети. В процессе разработки НС, будет применена самая распространённая функция, используемая как активационная функция нейронных сетей называемая сигмоидальной. Также следует отметить данная функция является быстро возрастающей и дифференцируемой, что отводит ей значимую роль в теории НС особенно в методе обратного распространения ошибки в сети вида многослойный персептрон [3].

Для архитектуры искусственной НС была выбрана двухслойная сеть со скрытыми слоями, первый слой состоит из 41 нейрона, именно столько признаков сетевых атак на данные мы вывели, исследуя предметную область. Второй слой состоит из 21 нейрона, что соответствует количеству возможных вариантов атак, выявленных нами при анализе информационный базы. И результирующий слой из двух нейронов, отвечающих за информирование наличия атаки или её отсутствия.

Обучения нейронной сети. Для обучения разрабатываемой нами НС был выбран метод обратного распространения ошибки. Выбранный метод обучения обеспечивает построение аппроксимации для траектории в пространстве весов. Для построения более гладкой траектории в пространстве весов, нужно уменьшить параметр скорости обучения, что приведёт к меньшей корректировке значений синоптических весов, осуществляемой на каждой итерации. Так как улучшение приводит к снижению скорости обучения, то простейшим способом её повышения является изменение дельта-правила (*метод обучения перцептрона по принципу градиентного спуска по поверхности ошибки. Его дальнейшее развитие привело к созданию метода обратного распространения ошибки*), добавив к нему момент итерации, что приведёт к повышению скорости обучения без потери устойчивости [1].

Обучение НС в нашем случае представлено в виде задачи глобальной оптимизации, где метод обратного распространение ошибки принимает форму градиентного спуска, иначе говоря спуска по поверхности ошибки, корректируя веса в направлении минимума. В сложных сетях поверхность ошибок сильно искривлена и состоит из различных холмов, долин, складок и ущелий в высокоразмерном пространстве, что может привести к попаданию сети в локальный минимум, даже если рядом находится более глубокий минимум, проблема в том, что в локальном минимуме все направления направлены вверх, и сеть не может оттуда выйти. Данная проблема является сложной часть обучения НС, а именно в поиске выхода из локального минимума. При каждом выходе из локального минимума, она ищет следующий локальный минимум, используя тот же метод обратного распространения ошибки, пока не будет найден выход. Данный процесс снижает точность вычислений и увеличивает вероятность остаться в локальном минимуме, поэтому для нахождения парильного решения необходимо использовать эвристические алгоритмы оптимизации.

Результаты. Для анализа эффективности работы предложенной методики нами был разработан программный комплекс, состоящий из процессов обучения нейронной сети различными методами и модулей тестирования полученных результатов. Данный проект состоит из нескольких основных функциональных блоков:

– *Блок настройки параметров сети,* позволяющий производить ввод начальных параметров роя частиц, а также параметров самой нейронной сети;

– *Блок загрузки базы данных сетевых атак*. База данных подгружается из вне, так как она является результатом работы одного из ведущих университетов, то в изначальном виде представляет избыточные данные, поэтому были разработаны модули работы с подгружаемыми данными;

– Основной блок программы, позволяющий обучать создаваемую НС и тестировать её на количество ложных срабатываний и точность вычислений. Также был

реализован блок обработки результатов для перезаписи полученных синаптических весов в процессе обучения.

В проверки точности работы НС, был проведён сравнительный анализ на нескольких сгенерированных нейронных сетях с разным количеством пройденных примеров. Результаты показали, что среднеквадратичная ошибка и скорость сходимости улучшаются пропорционально количеству пройденных примеров, но процесс обучения методом роя частиц гораздо выше, чем у метода обратного распространения ошибки.

Заключение. Предложенная методика обучения нейронной сети методом роя частиц значительно повышает точность результата работы обучаемой сети и уменьшает количество ложных срабатываний. Использовав данный метод, была достигнута оптимальная настройка обучения нейронной сети, что позволяет использовать данный методику в практической деятельности.

Перечень используемой литературы и источников:

1. Искусственные нейронные сети и приложения: учеб. пособие / Ф.М. Гафаров, А.Ф. Галимянов. – Казань: Изд-во Казан. ун-та, 2018. – 121 с.
2. Artificial-intelligence-particle-swarm-optimization. [Электронный ресурс]. – URL: https://learn.microsoft.com/ru-ru/archive/msdnmagazine/2011/august/artificial-intelligence-particle-swarm-optimization (Дата обращения: 21.03.23).
3. Хайкин С. Нейронные сети. Полный курс. Второе издание. – Москва: ИД «Вильямс», 2006. – 1104 с.
4. Y. Shi, R. Eberhart. A modified particle swarm optimizer // The 1998 IEEE International Conference on Evolutionary Computation Proceedings. 1998. – Pp. 69-76.

ГЛАВА 2.
ПРОБЛЕМЫ ИНФОРМАЦИОННОЙ БЕЗОПАСНОСТИ

2.1. АНАЛИЗ НЕДОСТАТКОВ ТЕХНОЛОГИЙ ОБНАРУЖЕНИЯ И РАССЛЕДОВАНИЯ ИНЦИДЕНТОВ БЕЗОПАСНОСТИ

Рассматриваются современные решения для мониторинга и предотвращения информационных угроз. Сделан обзор основных технологий информационной безопасности (ИБ), предназначенных для выявления угроз на разных уровнях. Затронуты этапы реагирования на инциденты информационной безопасности и описаны способы решения для них. Проанализированы основные недостатки технологий обнаружения и расследования инцидентов безопасности.
Ключевые слова: инцидент, идентификация, информационная безопасность, инциденты безопасности, кибератака, обнаружение, сигнатура.

ANALYSIS OF DISADVANTAGES OF SECURITY INCIDENT DETECTION AND INVESTIGATION TECHNOLOGIES

Modern solutions for monitoring and preventing information threats are considered. An overview of the main information security (IS) technologies designed to identify threats at different levels is given. The stages of responding to information security incidents are touched upon and solutions for them are described. The main shortcomings of technologies for detecting and investigating security incidents are analyzed.
Keywords: incident, identification, information security, security incidents, cyber-attack, detection, signature.

Введение. Кибератаки постоянно совершенствуются как по сложности, так и по масштабам. Важно использовать соответствующие решения, которые усиливают защиту инфраструктур, будь то локальных, облачных или гибридных. В отличие от большинства кибератак, не несущих за собой долгосрочную проблему, имеются более продвинутые постоянные угрозы, для которых требуются решения, ориентируемые на выявление целевых атак и сложных угроз, например таких, как APT (от англ. Advanced Persistent Threat – Развитая устойчивая угроза) [1, 2, 12].

В большинстве своем субъект угрозы пытается использовать один эксплойт или механизм для компрометации как можно большего числа узлов и стремится как можно скорее получить прибыль от злоупотребления полученной информацией. Однако в атаках APT угрожающий субъект предпочитает оставаться в тени, используя более сложные методы вторжения, и продлить контроль над взломанными узлами [2, 13].

Разнородность атак создает множество проблем для традиционных механизмов безопасности. Например, из-за своего скрытного характера APT обходят антивирусы, поэтому для их своевременного обнаружения необходимы более совершенные методы. При этом они не могут полностью заменить антивирусы из-за того, что решают конкретно свои задачи.

Каждый класс решений систем информационной безопасности (ИБ) взаимодействует с угрозами на разном уровне. Так, один метод обеспечивает защиту конечных устройств, другой же осуществляет сбор и анализ информации в сети, а третий может обеспечивать работу на разных уровнях инфраструктуры, но иметь очень узкую совместимость с другими решениями. Каждый из них обладает своими преимуществами или недостатками, и чтобы это компенсировать их используют вместе.

Обзор методов обеспечения ИБ конечных устройств. EPP (от англ. Endpoint Protection Platform – платформа защиты конечных точек) – это набор программных инструментов и технологий, которые служат для защиты устройств от угроз. Основной

механизм защиты конечной точки заключается в сопоставлении сигнатур угроз, уже хранящихся в базе данных, чтобы определить, является ли она вредоносной или нет [3].

EPP, как и традиционное антивирусное программное обеспечение, имеет полную функцию идентификации сигнатур. Для этого существует база данных с сигнатурами вирусов. Процедура идентификации основывается на различных алгоритмах, которые могут отличаться в зависимости от компании-изготовителя. Обнаружение, основанное на сигнатурах, является наиболее распространенным методом при защите от вторжения. Он является важной частью EPP. Это процесс мониторинга событий и анализ их на наличие признаков вторжений, происходящих в компьютерной системе или сети.

При этом метод имеет такие недостатки, как уязвимость к атакам нулевого дня, высокий процент ложных срабатываний и сложность реагирования на атаки, обходящие обнаружение [4]. Поэтому наряду с ними используют методы на основе проактивного обнаружения.

EDR (от англ. Endpoint Detection and Response – обнаружение и реагирование на конечной точке) – это технология, которая была разработана для преодоления недостатков поведенческих методов обнаружения. EDR поддерживается в различных операционных системах и разрабатывается с использованием открытых источников, что улучшает сотрудничество экспертов по всему миру и позволяет им быстрее подготавливать ответные меры на новые методы атак. Стоит отметить, что он сочетает в себе непрерывный мониторинг в режиме реального времени и сбор данных с автоматическим реагированием.

Обычно архитектура состоит из нескольких клиентов, которые посылают данные серверу, а он, в свою очередь, сравнивает их. Инструменты EDR постоянно отслеживают действия на устройствах и предупреждают об угрозе, если замечено потенциально вредоносное поведение. В отличие от сигнатурного сканирования или методов обнаружения аномалий, инструменты EDR ищут угрозы, сопоставляя системные события с базой знаний вражеских тактик, техник и процедур [5].

Данная технология была предложена Антоном Чувакиным для описания новых систем безопасности, которые обнаруживают и расследуют подозрительную активность на хостах и конечных точках, применяя автоматизацию, чтобы позволить командам безопасности быстро выявлять угрозы и реагировать на них.

Конечные точки включают компьютеры, серверы, планшеты, смартфоны, устройства Интернета вещей. Каждое устройство является потенциальной точкой входа для кибератак. Следовательно, их видимость и защита являются критически важными. EDR предоставляет собой централизованную и интегрированную платформу для сбора, корреляции и анализа данных, а также для координации немедленного оповещения об угрозах и реагирования, и имеет следующие основные функции [5]:

- мониторинг и сбор данных о потенциальных угрозах;
- анализ данных и выявление вредоносных шаблонов;
- автоматическое реагирование на выявленные угрозы путем их удаления или остановки, отправка предупреждающих уведомлений;
- инструменты анализа для сканирования на предмет выявленных угроз и обнаружения подозрительных действий.

Этим технологии не ограничились. В попытках создать более интегрированную систему, был придуман следующий класс решений. XDR (от англ. Extended Detection and Response – расширенные обнаружение и реагирование) – это подход к обнаружению угроз и реагированию на них, обеспечивающий глобальное и прямолинейное представление всего технологического охвата. Таким образом, он обеспечивает видимость данных в сетях, облаках, конечных точках и приложениях, применяя аналитику и автоматизацию для обнаружения, анализа, поиска и исправления угроз [6].

Основным отличительным моментом XDR является сбор и корреляция данных из всей инфраструктуры, включая электронную почту, конечные точки, серверы, облачные рабочие нагрузки и сети, что обеспечивает глобальную видимость и расширенный контекст угроз. Таким образом, угрозы можно анализировать, определять их приоритетность, преследовать и устранять для предотвращения потери данных и нарушения безопасности. По мере увеличения видимости, а также контекста угрозы, события, на которые раньше не обратили бы внимания, могут быть соотнесены в единое целое, что позволяет командам безопасности выявить и устранить или смягчить серьезность и масштаб атаки.

XDR объединяет множество продуктов в целостную, единую платформу для обнаружения инцидентов безопасности и реагирования на них, развивая решения для обнаружения и реагирования на конечных точках [6].

Основными достоинствами XDR являются повышение эффективности систем безопасности, производительность операций и расширение возможностей обнаружения и реагирования за счет включения большего количества компонентов безопасности в единое целое, что предполагает более широкий спектр услуг, представляя возможности для различных форм обнаружения и одновременного использования нескольких методов реагирования. По своим функциям XDR схожи с системами SIEM (от англ. Security information and event management – управление информацией и событиями о безопасности) и SOAR (от англ. Security Orchestration, Automation and Response – управление безопасностью, автоматизацией и реагированием), однако XDR отличаются уровнем интеграции своих продуктов при развертывании, а также фокусом на обнаружения угроз и реагирования на инциденты. Хотя SIEM-решения применяют часто, но иногда ограничиваются только некоторыми возможностями, например используют для хранения журналов.

Продукты XDR направлены на решение основных проблем, связанных с продуктами SIEM, таких как эффективное обнаружение и реагирование на целевые атаки, включая встроенную поддержку анализа поведения, анализа угроз, профилирования поведения и аналитики. Поставщики SIEM, как правило, не имеют лабораторий по обнаружению угроз и анализу исследований такого же уровня, как поставщики XDR. Большинство продуктов XDR разрабатываются с использованием новых «облачных» технологий и сервисов, что делает их новой альтернативой или дополнением к существующим инструментам SIEM. Благодаря облачным технологиям, XDR также имеет потенциал для использования новых аналитических решений. Однако XDR не являются заменой для всех случаев использования SIEM, таких как общее хранение журналов или соответствие нормативным требованиям.

Основные этапы реагирования на инциденты ИБ. Реагирование на инциденты ИБ можно разделить на следующие этапы: подготовку, обнаружение, расследование, предотвращение. Для эффективного обнаружения, расследования и удаления вредоносного программного обеспечения необходимо учесть все возможные угрозы и использовать против них определенные решения. Пул технологий, который был установлен при подготовке, в дальнейшем сможет обеспечивать надежную защиту системы.

За отслеживание сигналов тревоги обычно отвечают SIEM-решения. Существует две отдельные области, которые совместно составляют SIEM, SIM («Security Information Management» и SEM («Security Event Management»). SIM отвечает за накопление, анализ и последующие представление зарегистрированных данных, которые представляют собой информацию от хост-систем, различных приложений, брандмауэров и антивирусов. SEM же связан с получением информации в реальном времени. В свою очередь, SIEM собирает и объединяет данные журналов организации, чтобы в дальнейшем идентифицировать, классифицировать и исследовать угрозы [7, 8].

Результаты анализа формируются в виде предупреждений и отчетов. В течение нескольких часов данные хранятся в SIEM в режиме онлайн, а затем перемещаются в архив. Существует два метода сбора данных. В первом случае, называемом Pull, SIEM пытается получить данные с исходного устройства или агента. Второй вариант называется Push, в его случае устройство передает журнал данных периодически. Подход Pull позволяет получить доступ к каждому устройству, поэтому является более значимым. Процесс корреляции включает в себя объединение различных событий журнала для создания картины инцидента безопасности. Это довольно сложный процесс, поскольку требуется тщательная идентификация угроз.

При обнаружении угрозы система должна оповестить пользователя или сотрудника об инциденте безопасности. Это может происходить тремя способами: либо об угрозе сообщается сразу после ее возникновения, либо через периодические отчеты, либо администратор активно проверяет SIEM в режиме реального времени, чтобы немедленно получить информацию о любой угрозе. После сотрудник должен проверить, является ли инцидент ложным или нет. Отчеты же могут быть составлены по заранее определенными шаблонам. Если угроза является реальной, то аналитикам потребуется быстрый доступ ко всем данным с конечных точек и к информации об активностях, чтобы провести глубокий анализ источников угроз.

SIEM-решения используют для анализа всей сети в целом, а сбор данных со всех устройств очень затратно. Поэтому кроме них используют и EDR-технологии, которые затрагивают более глубокие угрозы. EDR может в общей системе взаимодействовать с SIEM, отправляя ему данные, а она, в свою очередь, обрабатывает их и оповещает оператора. SIEM предоставляет более удобный интерфейс и позволяет аналитикам писать длинные специальные запросы для объединения этапов атаки, при условии, что у них есть опыт и знания для этого.

Как уже было упомянуто ранее, при обнаружении EDR технология выявляет атаки, основываясь на базе данных известных тактик злоумышленников. Для этого она сравнивает логи с огромной базой данных MITRE ATT&CK (от англ. Adversarial Tactics, Techniques & Common Knowledge – тактики, техники и общеизвестные факты о злоумышленниках). Матрица MITRE ATT&CK [9] – это общедоступная база знаний об вражеских тактик, техник и процедур, которая курируется экспертами в данной области на основе анализа реальных атак APT, и является одной из наиболее широко используемых коллекций. Одни из лучших инструментов EDR используют именно эту базу знаний для обнаружения поведения противника [2].

Обнаружение является важной частью защиты конечных точек, но иногда все равно происходят ситуации, когда вирусы заражают систему или сеть через устройство. Организации должны исключить любую возможность вторжения через него, чтобы обеспечить безопасность своей системы. EPP направлен на устранение вируса, который попал на устройство и может нанести системе значительный ущерб. Если какое-либо программное обеспечение или файл считаются вредоносными, то они сразу заносятся в черный список. Для удаления угрозы технология EPP использует алгоритм HIDS (от англ. Host-based intrusion detection system – хостовая система обнаружения вторжений), он отслеживает подозрительные действия и собирает характеристики клиентов и серверов [10]. Если же другие устройства в системе заразились, то EDR решения могут обеспечить сканирование каждого из них, благодаря динамическому мониторингу всех конечных точек, что предотвратит дальнейшее заражение системы.

Каждое рассмотренное решение применяется либо на уровне сети, либо на уровне конечной точки и может пользоваться независимо друг от друга. Но XDR инструменты реализуются на всей инфраструктуре, что повышает эффективность операций по обеспечению безопасности. Он собирает и фильтрует различные потоки телеметрии, анализируя тактики, методы и другие типы угроз, чтобы упростить использование оперативных ресурсов безопасности. Все это дает аналитикам больше

информации по обнаружению и расследованию атаки и позволяет блокировать угрозы, используя аналитику на основе искусственного интеллекта и поведенческой защиты от угроз.

Уязвимости технологий обнаружения и расследования инцидентов безопасности. Несмотря на то, что современные антивирусные решения могут идентифицировать и блокировать угрозы, множество инструментов безопасности, работающие независимо друг от друга, усложняют процесс обнаружения и предотвращения атак, особенно если они дублируют друг друга и генерируют одинаковые предупреждения.

При использовании EDR-решений стоит отметить и его недостатки. По большей части проблемой может послужить использование базы знаний матрицы MITRE ATT&CK. Она заключается в том, что некоторые процедуры, которые могут быть связаны с атакой, используются и для безобидных целей. Одним из примеров может послужить удаление файлов, что может указывать как на присутствие атаки APT, так и на обычную деятельность пользователя. Также инструменты EDR собирают множество полезной контекстной информации, среди которой могут быть запущенные процессы и сетевые соединения. Но при их анализе необходимо вручную собрать воедино цепочку системных событий. Если предупреждение считается действительно подозрительным, аналитик должен восстановить и соотнести различные этапы атаки путем дальнейшего изучения огромных системных журналов. Исходя из этого EDR решения страдают от трех проблем:

1) инструменты EDR генерируют большое количество ложных тревог, что приводит к задержкам в выполнении задач по расследованию.

2) определение достоверности этих предупреждений об угрозах требует утомительного ручного труда из-за огромного количества низкоуровневых системных журналов, что создает проблемы для аналитиков.

3) из-за огромного ресурсного бремени, связанного с хранением журналов, на практике системные журналы, описывающие долговременные кампании атак часто удаляются еще до начала расследования.

SIEM технология в свою очередь является очень узкоспециализированной и не имеет столько же возможностей, но очень часто используется вместе с другими инструментами. В модели SIEM можно выделить следующие проблемы [8]:

1) интеграция SIEM требует больших усилий. Кроме того, трудно создать стандартное решение, пригодное для использования несколькими компаниями.

2) имеется спрос на специалистов. Несмотря на то, что потребность в персонале снижается, все еще существует необходимость в экспертах для внедрения и мониторинга системы.

3) недостаток информации из наблюдений, сделанных людьми. В шаблоне используются только журнальные и контекстные данные, генерируемые машинами.

Однако люди также могут предоставить ценную информацию для SIEM. Например, если сотрудник получает вредоносный телефонный звонок, который может стать началом крупномасштабной атаки, у него нет возможности передать его в систему SIEM.

4) SIEM предназначена только для обнаружения и анализа угроз и не имеет функций для реагирования на них.

EPP является хорошей защитой для конечных устройств, но при устранении передовых методов взлома возникают недостатки. Иногда сигнатуры вирусов не могут быть сопоставлены вовремя, поскольку потенциальные угрозы обновляются достаточно часто, особенно при нацеленной атаке. Поэтому в средствах EPP обычно выделяют следующие проблемы: чрезмерное использование ресурсов, метод обнаружения на основе сигнатур, требование интернета как обязательное условие для

выполнения многих функций и невозможность защититься от внутренних угроз, когда вирус уже проник в сеть.

XDR содержит в себе большинство функциональных возможностей других технологий, но она находится только на стадии формирования. Это решение может повысить эффективность безопасности, но при этом оно чаще всего специализировано в одном направлении, и кроме этого, вполне возможно наличие слабой стороны защиты в конкретном продукте, так что при попытке реализовать дополнительные функции могут произойти ошибки, следовательно имеются проблемы с совместимостью других инструментов, которые могли бы показать большую эффективность в своем классе.

Заключение. Системы информационных технологий всегда подвержены риску, однако организации не всегда готовы предложить надлежащий ответ на инциденты безопасности. Поэтому имеется высокая необходимость в четких вариантах реагирования на них. Устройства также могут стать целью заражения и потенциальной атаки. Но имеется множество способов для их защиты [11].

Некоторые функциональные возможности решений пересекаются, но из-за своих особенностей они не могут максимально эффективно защитить систему, работая независимо друг от друга. Были представлены методы, позволяющие автоматизировать обнаружение и расследование инцидентов безопасности и предоставляющие удобные инструменты для анализа журнала угроз высококвалифицированными сотрудниками. Для более эффективной защиты инфраструктуры требуется совместное использование технологий обнаружения и реагирования. Поставщики услуг учитывают этот факт, поэтому предоставляют все необходимые инструменты. Несмотря на выявленные недостатки рассмотренных технологий, каждое из решений повсеместно пользуется в разных компаниях. Существуют и сложности при интеграции продуктов безопасности. Учитывая выявленные недостатки, становится ясно, что необходимо внедрение упрощенных решений, которые позволят иметь глобальный взгляд на инфраструктуру и все его приложения.

Перечень использованной литературы и источников:

1. Ермаков А.О., Кавешников М.Б., Клянчина Е.В. Вредоносное программное обеспечение APT-групп и его характеристики // Вопросы кибербезопасности. – 2017. - № S2(20). – С. 24-29.
2. Karantzas G., Patsakis C. An empirical assessment of endpoint detection and response systems against advanced persistent threats attack vectors / C. Karantzas, C. Patsakis // Journal of Cybersecurity and Privacy. 2021. Vol. 1. №. 3, pp. 387-421.
3. Chandel S. Endpoint protection: Measuring the effectiveness of remediation technologies and methodologies for insider threat // 2019 international conference on cyber-enabled distributed computing and knowledge discovery (cyberc). 2019, pp. 81-89.
4. Galal H.S., Mahdy Y.B., Atiea M.A. Behavior-based features model for malware detection // Journal of Computer Virology and Hacking Techniques. 2016. Vol. 12. №. 2, pp. 59-67, May 2016.
5. Hassan W. U., Bates A., Marino D. Tactical provenance analysis for endpoint detection and response systems // 2020 IEEE Symposium on Security and Privacy (SP). 2020, pp. 1172-1189.
6. Jauhiainen H. Designing End User Area Cybersecurity for Cloud-based Organization. 2021. P. 52.
7. Chopra M., Mahapatra C. Significance of security information and event management (SIEM) in modern organizations // International Journal of Innovative Technology and Exploring Engineering. 2019. Vol. 8. №. 7, pp. 432-435.
8. Vielberth M., Pernul G. A security information and event management pattern // 12th Latin American Conference on PatternLanguages of Programs. 2018. P. 12.
9. Strom B.E. Mitre att&ck: Design and philosophy // Technical report. The MITRE Corporation. 2018. P. 36.
10. Liao H. J. et al. Intrusion detection system: A comprehensive review // Journal of Network and Computer Applications. 2013. Vol. 36. №. 1, pp. 16-24.
11. Anwar S. From intrusion detection to an intrusion response system: fundamentals, requirements, and future directions // Algorithms. 2017. Vol. 10. №. 2. P. 39.
12. Крейнделин В. Б., Легков Н.А. Защита аутентификационных данных сайтов и WEB-приложений // Телекоммуникации и информационные технологии. – 2022. Т. 9. - № 1. – С. 6-10.
13. Крейнделин В.Б., Авидзба А.Д. Шифрование Wi-Fi protected access // Технологии информационного общества: XI Международная отраслевая научно-техническая конференция: сборник трудов, Москва, 15-16 марта 2017 года. – Москва: Медиа паблишер, 2017. – С. 294.

2.2. К ВОПРОСУ О ОБЕСПЕЧЕНИИ ИНФОРМАЦИОННОЙ БЕЗОПАСНОСТИ ГОСУДАРСТВЕННЫХ ИНФОРМАЦИОННЫХ РЕСУРСОВ

В данной статье рассматривается проблема обеспечения информационной безопасности (ИБ) государственных информационных ресурсов, выявляются основные риски, освещаются основные факторы, определяющие риски.
Ключевые слова: государственные информационные ресурсы (ГИР), информационная безопасность (ИБ) в государственной сфере, определение рисков, сети связи общего пользования (ССОП), центр обработки данных (ЦОД).

ON THE ISSUE OF ENSURING INFORMATION SECURITY OF STATE INFORMATION RESOURCES

This article examines the problem of ensuring information security (IS) of government information resources, identifies the main risks, and highlights the main factors that determine the risks.
Keywords: state information resources (GIR), information security (IS) in the public sphere, risk identification, public communication networks (PCN), data processing center (DPC).

Защита информации в современном мире – это та сфера, где всем организациям следует придерживаться единым принципам на основе государственных законов.
Путин В.В.
Президент Российской Федерации

Государство в процессе своей деятельности формирует государственные информационные ресурсы (ГИР), которые являются его собственностью и обязаны, за исключением случаев информации, составляющей государственную тайну и конфиденциальной информации, предоставляться в публичный доступ без ограничений посредством информационно-телекоммуникационных сетей. Это положение зафиксировано на уровне законодательства, в частности, Федеральным законом от 27 июля 2016 года № 149-ФЗ «Об информации, информационных технологиях и о защите информации» [1].

Граждане в абсолютном своём большинстве получают доступ к государственным информационным ресурсам посредством глобальной сети «Интернет». Порядок доступа к государственным информационным ресурсам посредством сети «Интернет» законодательством не определен. Ст. 15 149-ФЗ в редакции от 19.12.2016 года явно указывает на необходимость использования отраслевого законодательства [3], в частности, Федерального закона от 07 июля 2003 года № 126-ФЗ «О связи». Однако, закон «О связи» не выделяет среди видов информационно-телекоммуникационных сетей такую сущность как «сеть Интернет» [2]. По своей технической сути «сеть Интернет» является частью сети связи общего пользования (ССОП) со всеми вытекающими из этого последствиями для технической реализации доступа к государственным информационным ресурсам, методам и средствам обеспечения информационной безопасности. Следует отметить, что в связи с техническими особенностями построения ССОП, высококонкурентной средой в отрасли, высокой степенью фрагментации технологий, организационных и технических средств обеспечения управления сетями связи, входящими в ССОП, единых подходов к обеспечению информационной безопасности ССОП нет.

Таким образом, исследуя вопросы обеспечения информационной безопасности государственных информационных ресурсов, необходимо рассматривать в качестве источника угроз и объекта защиты ССОП, как один из элементов инфраструктуры государственного информационного ресурса.

Впрочем, ГИР, помимо ССОП, обладает более сложной и иерархической инфраструктурой, в которой целесообразно выделять локальную сеть центра обработки данных (ЦОД), вычислительное оборудование, системы хранения данных, системное и базовое прикладное программное обеспечение. Причем, вычислительное оборудование и программное обеспечение целесообразно объединить термином вычислительная инфраструктура. Это справедливо на высоком уровне абстракции от конкретной реализации ГИР.

В части касающейся конкретных реализаций инфраструктуры и программно-технических архитектур ГИР и их компонентов, наблюдается высокая степень фрагментации, что говорит об отсутствии единой технической политики и предопределяет индивидуальные решения в области обеспечения информационной безопасности ГИР и их компонентов.

Дополнительную негативную тенденцию во фрагментацию инфраструктур и технического исполнения ГИР вносят децентрализованные полномочия ведомств на федеральном и региональном уровнях государственного управления.

Невозможно обойти вниманием исполнение ГИР и обеспечивающих их аппаратных и программных комплексов и систем, построенных на импортной аппаратной и программной базе, что обуславливает импортозависимость ГИР в целом и подверженность киберугрозам, как технического, так и организационного характера, в том числе применением международных санкций.

В соответствии с действующими приказами регуляторов в области обеспечения ИБ, на сегодняшний день система обеспечения ИБ как отдельный, единый и централизованный контур управления безопасностью ГИР выстроен быть не может в силу приведенных выше аргументов о высокой степени фрагментации и отсутствию единой технической политики при построении ГИР.

Одновременно с этим, следует считать государственные органы заинтересованными в обеспечении установленных качественных характеристик и показателей всех уровней инфраструктуры для обеспечения доступа к государственным информационным ресурсам с надлежащим качеством, при обязательном соблюдении требований к обеспечению ИБ. В итоге мы имеем упрощенную модель архитектуры ГИР, которая предполагает четыре взаимосвязанных уровня:

1. Сеть связи общего пользования.
2. Инфраструктура ЦОД (сетевая и инженерная).
3. Вычислительная инфраструктура.
4. Инфраструктура хранения данных.

Фрагментация всех уровней на техническом и организационном уровне не позволяет применять единые подходы и технологии обеспечения ИБ. Система обеспечения ИБ ГИР не выделена в отдельный надсистемный по отношению к ГИР компонент.

Качественные параметры предоставления ГИР для потребителей не установлены, а система их установления и контроля соответствия установленным значениям отсутствует.

С учетом изложенного выше, вполне логично сделать выводы о недостаточном на сегодняшний день обеспечении ИБ ГИР, особенно в свете усилившихся рисков и угроз устойчивости и защищенности ГИР со стороны организованных преступных сообществ и иностранных государственных структур, действующих похожими на преступные методы.

Перечисленные факторы довольно однозначно определяют риски в отношении обеспечения ИБ ГИР, а именно:

- риски нарушения установленного режима ИБ, за счет множества объектов воздействия на инфраструктуру ГИР из-за децентрализованной системы управления на

уровнях ССОП, инфраструктуры ЦОД, вычислительной инфраструктуры и инфраструктуры хранения данных;

- риски нарушения установленного режима ИБ за счет отсутствия единого центра управления и мониторинга состояния защищенности ГИР;

- риски неправомерного доступа к ГИР и обеспечивающей инфраструктуре, в том числе для добывания информации ограниченного распространения, за счет применения оборудования и программного обеспечения иностранного производства, слабо или вовсе не контролируемого уполномоченными органами РФ;

- экономические риски, связанные с многократным повторением технических решений не являющихся типовыми из-за отсутствия единой технической политики.

ФГБУ НИИ «Восход» в рамках научно-исследовательской работы «Гособлако», используя его результаты при выполнении государственного задания на 2016 год по тематике «Единая система центров обработки данных», в отраслевой кооперации с ПАО «Ростелеком», ООО «РТК-ЦОД», ООО «ИнфоТекс» ООО «НТЦ Веллинк» провело большой объем исследовательских и конструкторских работ. Значительная часть работ была нацелена на разработку законодательных, нормативных, технических требований и апробацию конкретных технических решений для снижения рисков в отношении обеспечения информационной безопасности ГИР. В кооперации с «ИнфоТекс» и «Центром безопасности информации» разработаны концептуальные подходы к реализации выделенной подсистемы обеспечения информационной безопасности. Результатом выполнения работ в контексте рассматриваемых рисков явились:

- разработанная архитектура системы распределенных вычислений с единым центром мониторинга и управления, в том числе, функционирующие в особые периоды. Особенностью архитектуры является явное выделение системы обеспечения ИБ всех уровней в отдельную инфраструктуру с собственными регламентами взаимодействия и реагирования на инциденты. Еще одной особенностью архитектуры является апробация возможности применения сетевого оборудования, серверного оборудования и систем хранения данных отечественного производства, равно как и системы управления виртуализацией;

- разработанные проекты нормативных правовых актов обязывают владельцев ГИР разместить их в единой системе ЦОД, обеспеченной единой технической политикой, методическим обеспечением процесса миграции в единую инфраструктуру, обеспеченную отдельным компонентом обеспечения ИБ, предусматривающий интерфейсы взаимодействия с ГосСОПКА в том числе. Со стороны ССОП, принимая во внимание невозможность в обозримые сроки реализации централизованной системы управления сетью связи, рассматривались в дополнение исключительно угрозы использования ССОП для организации атак на отказ в обслуживании компонентов архитектуры. В практическом плане мониторинг и подавление атак осуществлялось программно-аппаратным комплексом, аналогичным «Arbor Peakflow SP», российского производства на сети оператора связи «Информика» (См. Рис .1)

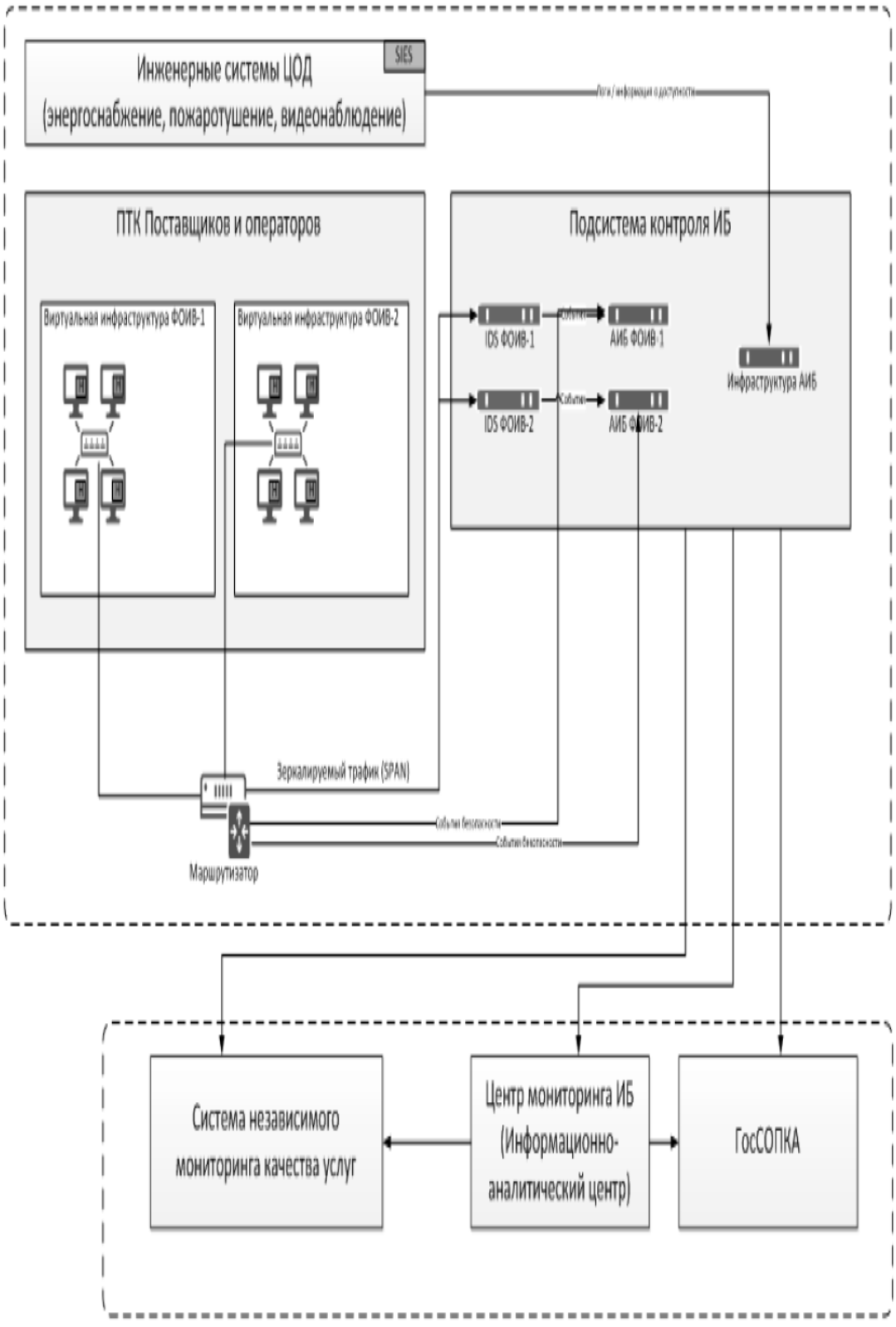


Рисунок 1 – Общая схема компонента обеспечения ИБ единой системы ЦОД

Отдельно следует упомянуть работу, завершенную Общественно-государственным объединением «Ассоциация документальной электросвязи» по разработке «Концепции управления качеством на сетях электросвязи», которая была представлена отраслевому регулятору в начале 2016 года. Эксперты ФГБУ НИИ «Восход» обеспечили включение в состав концепции положений, закрепляющих за

уполномоченным в области информационных технологий и связи государственным органом установление требований к операторам связи по обеспечению качественных показателей доступа к ГИР. Что, в случае принятия и исполнения «Концепции …» приведет к необходимости со стороны операторов выполнения комплекса организационных и технических мероприятий, вязанных, в том числе, с компьютерными атаками на ССОП с целью ухудшить параметры доступа потребителей ГИР или блокирования доступа к ГИР. В целях обеспечения государственного контроля разработана «сквозная» для всех уровней система мониторинга показателей, «бесшовно» интегрированная с системой управления.

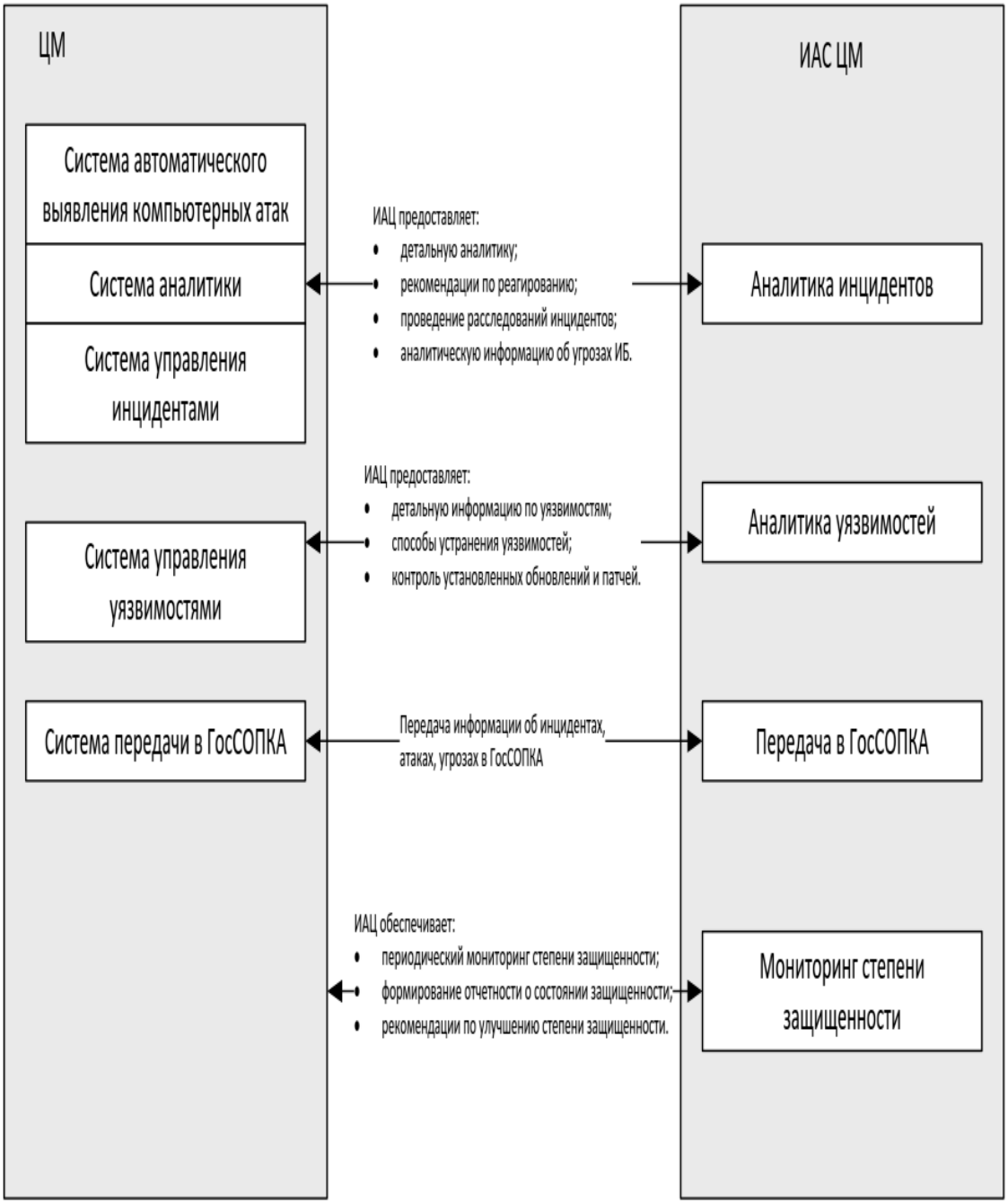


Рисунок 2 – Схема взаимодействия
с информационно-аналитическим центром

Таким образом, в ходе выполнения работ предложены и апробированы конкретные архитектурные и технические решения, разработаны проекты нормативных документов и нормы технического регулирования, позволяющие минимизировать риски, связанные с текущим состоянием защищенности ГИР.

Перечень использованной литературы и источников:
1. Российская Федерация. Законы. Об информации, информационных технологиях и о защите информации: федер. закон от 27 июля 2016 года № 149-ФЗ // СПС «КонсультантПлюс».
2. Российская Федерация. Законы. О связи: федер. закон от 7 июля 2003 года № 126-ФЗ // СПС «КонсультантПлюс».
3. А.Н. Прокопенко, А.А. Кривоухов. Правовая политика Российской Федерации в сфере государственных информационных ресурсов // Научные ведомости. – 2007. - №9. – С. 173-182.

2.3. АНОНИМИЗАЦИЯ И ДЕАНОНИМИЗАЦИЯ ПОЛЬЗОВАТЕЛЕЙ ИНТЕРНЕТ-ПОРТАЛОВ И СОЦИАЛЬНЫХ СЕТЕЙ В ЦЕЛЯХ ОБЕСПЕЧЕНИЯ ИНФОРМАЦИОННОЙ БЕЗОПАСНОСТИ

Идентификация пользователей имеет решающее значение для большинства веб-сайтов, с целью предоставления таргетированного контента, либо для отслеживания злоумышленников Проанализированы подходы к идентификации и отслеживания работы пользователей социальных сетей на веб-ресурсах на основе анализа цифровых отпечатков устройств. Показано, что основной проблемой деанонимизации web-браузера является эволюция цифровых отпечатков устройств во времени, которая может быть преодолена путем разработки адаптивной интегрируемой системы.
Ключевые слова: атрибуты, база данных, браузер, идентификация, машинное обучение, фингерпринт, цифровые отпечатки.

ANONYMIZATION AND DEANONIMISATION OF USERS OF INTERNET PORTALS AND SOCIAL NETWORKS FOR THE PURPOSES OF ENSURING INFORMATION SECURITY

Identification of users is crucial for most websites in order to provide targeted content, or to track intruders. Approaches to identifying and tracking the work of social network users on web resources based on the analysis of digital fingerprints of devices are analyzed. It is shown that the main problem of web browser de-anonymization is the evolution of digital fingerprints of devices over time, which can be overcome by developing an adaptive integrated system.
Keywords: attributes, database, browser, identification, machine learning, fingerprint, digital prints.

Актуальность задачи: Задача деанонимизация пользователей важное значение для обеспечения национальной безопасности. Более 90% наиболее популярных сайтов в Интернете осуществляют сбор информации о пользователях в автоматизированном режиме. В процессе сбора данных формируется профиль человека, который способен содержать в себе: пол (мужчина, женщина); возраст; семейное положение; политические взгляды; финансовое состояние; интересы; привычки и т.д. Однако, остальные могут передавать эти цифровые отпечатки рекламным компаниям, с целью показа таргетированной рекламы.

В целях предотвращения использования своей персональной информации третьими лицами и недопущения их идентификации как физического лица некоторые пользователи (акторы) социальных сетей используют различные методы сокрытия своего авторства, получившие название методов анонимизации.

Вместе с тем подобная анонимизация пользователей может использоваться третьей стороной, например, для организации акций деструктивного характера.

Для предотвращения противоправных действий и идентификации пользователей используются отпечатки цифровых устройств.

Методы анонимизации и деанонимизации. Среди основных методов анонимизации можно выделить web-анонимайзеры, механизмы так называемой «луковой» маршрутизации TOR, сети I2P, VPN-туннели. Современное отечественное законодательство стремится ограничить применение анонимайзеров, а также повсеместно идентифицировать пользователей сети Интернет для повышения общего

уровня безопасности. В целом можно выделить следующие принципы анонимизации браузера: данные с низкой энтропией могут вообще не нуждаться в защите, а если защита производится, следует подменять параметр на максимально распространённое значение, не придавая ему искусственную нестандартность.

Известным способом отследить человека в Интернете является использование IP-адреса, с помощью которого можно отслеживать, какие онлайн-ресурсы посещает пользователь. Его аккаунты и геолокацию.

Каждый раз, когда пользователь посещает веб-страницу через Tor, злоумышленник записывает сетевую трассировку, например, перехватывая трафик локально, имея доступ к маршрутизаторам пользователя ISP, или контролируя защиту входа в сеть Tor. Затем он запускает классификатор по перехваченной сетевой трассировке, чтобы предположить сайт, которые посещал пользователь.

Наиболее распространенным способом идентификации и отслеживания работы пользователей на веб-ресурсах являются HTTP-cookies, часто устанавливаемые с помощью сторонних аналитических и рекламных сервисов [3]. В то же время, пользователь, стремящийся скрыть свою личность в Интернете, прибегает к способам фильтрации cookie до необходимых для функционирования пользовательского интерфейса, но не допускающих других видов отслеживания. В качестве механизма идентификации пользователей, ограничивающими cookie-файлы, используются методы снятия цифровых отпечатков браузеров и использование их как идентификатор конкретного пользователя.

Файлы «Cookie» - это небольшие фрагменты данных, отправляемые с веб-сайта и хранящиеся непосредственно в браузере. Любая информация может быть сохранена в файле cookie, но большинство из них содержат уникальный идентификатор, который ссылается на конкретную онлайн-идентичность. Например, когда пользователи заходят на свои любимые веб-сайты, файл cookie сохраняется для их идентификации и автоматического входа в систему при последующих подключениях. Информация, содержащаяся в файле cookie, позволяет веб-сайту проверять личность каждого пользователя по каждому запросу.

Поскольку цифровые отпечатки не оставляют никаких следов и наличия каких-либо меток на компьютере пользователя, а также являются пассивными и сложно обнаруживаемыми [4] они являются одним из возможных и вполне надежных способов деанонимизации пользователей, поскольку представляют собой набор уникальных значений, отражающих настройки web-обозревателя пользователя.

Под цифровым отпечатком устройства понимается информации, собранная web-сервером о вычислительном устройстве пользователя с целью уникальной идентификации устройства при последующих посещениях. В последние годы широкое распространение получило понятие *фингерпринт*.

Фингерпринтинг браузера – это методика отслеживания пользователей при помощи браузера [5]. Фингерпринтинг обеспечивает сбор данных о браузере пользователя, его системе и устройстве. Фингерпринтинг собирает такую информацию, как версия браузера, версия ОС, расширения, ход часов, GPU и CPU, разрешение монитора(ов) и размер окна браузера, шрифты, плагины, и прочее стороннее ПО. Разработчики браузеров, органы стандартизации долгое время пытаются бороться с этой проблемой, разрабатывая защитные средства от web-браузер фингерпринтинга, которые работают точечно и не мешают работе пользователя с браузером. Главная цель атакующего при web-браузер Фингерпринтинг – узнать, какую страницу посещает пользователь и какие действия он совершает.

Атакующему нужна эта информация для дальнейшего наблюдения или для разведывательных целей. Атаки такого типа обычно воспринимаются как проблема классификации, где категории классификации – веб-страницы, а наблюдения – следы трафика. Злоумышленник сначала собирает следы трафика, посещая веб-страницы и

обучает контролируемый классификатор с использованием таких функций, как длина, направление и время прибытия сетевых пакетов.

Цифровой отпечаток устройства может полностью или частично идентифицировать отдельных пользователей или устройства, даже когда cookie-файлы и другие средства отслеживания невозможны. Базовая информация о веб-браузере уже давно собирается веб-аналитическими службами с целью точного измерения реального веб-трафика и фильтрации автоматически созданных запросов.

Для того чтобы цифровой отпечаток можно было использовать в любой форме идентификации, собранная информация должна соответствовать двум ключевым принципам: уникальности и стабильности Уникальность требуется для того, чтобы обеспечить достаточную основу для идентификации. Каждый отпечаток должен быть как можно более уникальным. Это не обязательно означает, что каждый фрагмент собранной информации должен быть уникальным. Но комбинация всех атрибутов должна быть уникальной для конкретного устройства, чтобы обеспечить идентификацию. Свойство уникальности должно коррелироваться с размером набора данных и распределением популяции. Если сайт обрабатывает несколько тысяч соединений каждый день, число коллизий между отпечатками пальцев может быть очень низким или даже нулевым по сравнению с сайтом, обрабатывающим миллионы соединений.

Требование стабильности обусловлено следующим. По мере того, как пользователи обновляют свои устройства и настраивают свои браузеры, собранные отпечатки меняются. Для того чтобы связать отпечатки браузера, принадлежащие одному и тому же устройству, количество измененной информации должно быть как можно меньше. Например, сервер может время от времени ожидать обновления версии браузера, но изменение часового пояса более необычно, поскольку подразумевает, что пользователь путешествует. Различные типы поведения и различные типы изменений должны быть идентифицированы, чтобы иметь возможность идентифицировать устройство с точностью.

Контрмеры браузер фингерпринтинга. Контрмера – это решение, которое смягчает последствия снятия отпечатков пальцев в браузере. Большинство браузеров предоставляют встроенные меры по защите от межсайтового отслеживания. Учитывая, что разработчики браузеров предоставляют такие меры защиты от обычного отслеживания (например, cookie), те, кто заинтересован в идентификации пользователей, будут вынуждены использовать более жесткие меры, как браузер Фингерпринтинг. Исходя из этого, разработчики браузеров должны будут принимать меры по уменьшению влияния браузер фингерпринтинга.

Некоторые браузеры и инструменты для обеспечения безопасности пробовали уменьшить влияние браузер фингерпринтинга путем изменения информации API «JavaScript», которая отображается браузерами в Интернете. Например, браузеры, которые ориентированы на безопасность (например, Tor), ограничили доступ к таким API, как «Canvas» и «WebRTC», которые обычно использовали для реализации браузер фингерпринтинга. Однако при таком грубом запрете API нарушается функциональность сайтов, которые используют эти API в своей работе.

Таким образом, разработчики браузеров стараются избегать подобного подхода к блокировке API. В качестве альтернативного решения некоторые разработчики браузеров пробовали смягчить влияние браузер фингерпринтинга блокировкой сетевых запросов к сервисам браузер фингерпринтинга. Однако, и у этого метода есть свои недостатки: такой подход сильно полагался на ручной анализ и испытывал проблемы, когда дело доходило до запрещения скриптов, которые обслуживались собственными доменами или третьими лицами двойного назначения (например, CDN).

Существующие инструменты для защиты от отпечатков пальцев широко используют три разных подхода. Первый подход рандомизирует возвращаемые

значения API-интерфейсов «JavaScript», с которых можно снять фингерпринты. Второй нормализует возвращаемые значения API-интерфейсов «JavaScript», с которых можно снять фингерпринты. Третий использует эвристику для обнаружения и блокировки скриптов для снятия фингерпринтов.

У всех этих подходов есть достоинства и недостатки. Некоторые подходы защищают от активного снятия отпечатков пальцев, то есть скриптов, которые проверяют свойства устройства, такие как установленные шрифты, а другие защищают от пассивного снятия отпечатков пальцев, то есть серверов, собирающих, которая легко включается в веб-запросы, например, заголовок запроса «User Agent».

Подходы рандомизации и нормализации могут защитить от всех форм активного снятия отпечатков пальцев и некоторых форм пассивного (например, путем рандомизации заголовка запроса «User Agent»).

Подходы на основе эвристики могут защитить как от активного, так и от пассивного снятия отпечатков пальцев, например, путем полной блокировки сетевого запроса к ресурсу, который снимает фингерпринты.

Структура алгоритмов деанонимизации: Цифровые отпечатки устройств доказали свою полезность в реализации алгоритмов деанонимизации. Однако существует серьезная уязвимость данного вида идентификации. Цифровые отпечатки в следствие обновлений системы, плагинов, браузеров, установки различных программ, а с ними и шрифтов со временем изменяются, и, если сравнить два отпечатка одной системы в разные промежутки времени, можно увидеть различия обусловленные эволюцией цифровых отпечатков устройств. Однако поскольку эти различия как правило детерминированы, задачу идентификации анонимных пользователей возможно решить с помощью методов машинного обучения [6,7,8] путем разработки адаптивной интегрируемой системы. Математическая постановка задачи идентификации анонимных пользователей веб-ресурса на основе цифровых отпечатков устройств может быть сформулирована следующим образом. Пусть имеется множество источников цифровых отпечатков D $\{D1,\ldots,Dq\}$, где группа признаков для идентификации отдельных пользователей и некоторое конечное множество пользователей-кандидатов интернет-ресурса 1 { ,..., } *m U u u* . Измерение разнообразия отпечатков можно выполнить с помощью оценки энтропии H(T) $\sum_{I=1}..nP(tai)\ log_2\ P(t_{ai})$ где $T = \{t_a,\ldots,t_{an}\}$ - набор наблюдаемых признаков, а $P(t_{ai})$ дискретное распределение вероятности этих признаков. Если веб-ресурс регулярно посещает набор T различных браузеров с одинаковой вероятностью, то энтропия достигнет своего максимума и может быть оценена как 2 $H(T)$ log T.

В результате математическая постановка задачи идентификации пользователя сводится к нахождению такого набора признаков, который дает максимальную вероятность распознавания $P(Ta) – max\ Ta$ *где* $Ta = \{t_{a1}\ ,\ldots,\ tal\}$ – набор признаков максимизирующих вероятность распознавания. Используя полученные статистические данные, требуется выбрать набор признаков с максимальной энтропией и разработать алгоритм классификации а $t_{ux} – U$, способный идентифицировать пользователей U на основе цифрового отпечатка t_{ux}. Современные fingerprinting-методы могут даже не учитывать версию браузера, но всё равно распознавать конкретный ПК с высокой точностью за счёт особенностей его аппаратного обеспечения и операционной системы. Таким образом вопросы анонимизации и деанонимизация пользователей интернет-порталов и социальных сетей имеют важное значение для обеспечения национальной безопасности в краткосрочной и среднесрочной перспективе.

Проблемой деанонимизации пользователей социальных сетей является разработка алгоритмов, позволяющих провести массовую идентификацию пользователей путем использования дополнительных данных отдельных пользователей, извлекаемых путем анализа других социальных сетей.

Проблемой деанонимизации web - браузера является эволюция цифровых отпечатков устройств во времени, которая, однако может быть преодолена путем разработки адаптивной интегрируемой системы на основе методов машинного обучения и интеллектуальной обработки данных.

Перечень использованной литературы и источников:

1. Российская Федерация. Законы. О внесении изменений в Федеральный закон «Об информации, информационных технологиях и о защите информации»: федер. закон от 29.07.2017 № 276-ФЗ // СПС «КонсультантПлюс».
2. Башуев Я.П., Григорьев В.Р. Методы деанонимизации в социальных сетях // Я.П. Бушуев, В.Р. Григорьев // История и архивы. – 2016. - №3. – С.125-146.
3. Cookie. [Электронный источник]. – URL: https://techterms.com/definition/cookie 4. Identification of persons. [Электронный источник]. –URL: https://allegro.tech/2015/03/browser-fingerprints.html
5. Browser Fingerprint. Отпечаток браузера [Электронный источник]. – URL: https://www.youtube.com/watch?v=3D7HjYLkVrs
6. Шелухин О.И., Ерохин С.Д., Ванюшина А.В. Классификация IP-трафика методами машинного обучения / Под редакцией О.И. Шелухина. – Москва: Горячая-линия – Телеком, 2018. – 284 с.
7. Воробьева А.А., Позволенко В.А., Коробицына А.С., Шарафиев А.А. Межсайтовая лингвистическая идентификация интернет-пользователей // Научно-технический вестник информационных технологий, механики и оптики. – 2018. Т. 18. - № 3. – С. 447-456.
8. Шелухин О.И., Ванюшина А.В. Анонимизация и деанонимизация пользователей интернет-порталов: Учебно-методическое пособие по дисциплине «Интеллектуальные технологии информационной безопасности». – Москва: МТУСИ, 2021. – 47 с.
9. Шелухин О.И., Ванюшина А.В., Желнов М.С. Использование латентно семантического анализа при подготовке данных для идентификации анонимных пользователей по цифровым отпечаткам // Наукоемкие технологии в космических исследованиях Земли. – 2022. Т. 14. - № 1. – С. 36-44.
10. Шелухин О.И., Ванюшина А.В., Большаков А.С., Желнов М.С. Влияние эволюции цифровых отпечатков устройств на достоверность идентификации анонимных пользователей // Вопросы кибербезопасности. – 2022. - №2 (48). – С. 29-43.

2.4. ТЕЛЕФОННЫЙ ТЕРРОРИЗМ, КАК ФОРМА ПРОЯВЛЕНИЯ ЭКСТРЕМИЗМА

В данной статье авторы рассмотрели возможности расследования преступлений, связанных с телефонным терроризмом, которые осуществляют мошеннические действия. Приведены нормативно-правовые акты при расследовании данного вида преступлений.

Ключевые слова: МВД России, мошенничество, правовая ответственность за телефонный терроризм, преступление, терроризм, ущерб, хулиганство.

TELEPHONE TERRORISM AS A FORM OF EXTREMISM

In this article, the authors examined the possibilities of investigating crimes related to telephone terrorism that carry out fraudulent activities. The regulatory legal acts for the investigation of this type of crime are given.

Keywords. Ministry of Internal Affairs of Russia, fraud, legal liability for telephone terrorism, crime, terrorism, damage, hooliganism.

Уже сегодня люди живут в эпоху технического прогресса. Новейшие технологии захватывают наш быт. Специальная техника упрощает человеческую жизнь, делая её намного проще, комфортнее, интереснее и что не мало важно продуктивнее. Ведь с помощью техники можно выполнить самые тяжелые задачи для человека, она может то, на что не способен даже самый сильный или умный человек. Люди активно шагают вслед за прогрессом и теперь уже не могут представить свою жизнь без мобильного телефона, компьютера, планшета, телевизора, стиральной машины, а также различной кухонной техники такой как, например, комбайн или же блендер, посудомоечная машина или кофемашина и так далее. Кто бы мог подумать, что всё вышеперечисленное совсем недавно относилось к элементам роскоши и достать это простым людям было почти не реально, а сейчас пускай не всё, но всё же часть этого есть абсолютно в каждом доме. Такая техника стала просто необходимой для

комфортного проживания.

Прогресс сегодня значительно опередил прошлый век. Это повлияло на активное совершенствование науки и развитие человеческого мозга. Наша эпоха знаменуется передовыми технологиями и эффективным производством.

Мнение людей по поводу развития современной технологии расходятся. Одни считают, что это хорошо, другие твердят, что плохо.

Хотелось бы сначала сказать о положительной стороне технического прогресса. Первое и, наверное, самое важное на мой взгляд это совершенствование знаний, навыков и техники в медицине. Ничто не может быть более значимым, чем здоровье людей или животных. Развитие в медицине благоприятно повлияло на повышение продолжительности жизни, дало возможность в изучении ранее неизлечимых болезней или усовершенствование ранее изученных вакцин, болезней или патологий.

Теперь не нужно проводить кучу своего времени в библиотеках в поисках полезной и нужно информации для написания различных сочинений, докладов, рефератов, курсовых работ или дипломных. С помощью интернета это можно сделать в любом удобном месте, где есть возможность выйти в сеть. Поиск информации стал значительнее удобнее, тем самым колоссально экономя время.

Кроме этого, технический прогресс упростил работу по дому. Трудно представить современную кухню без микроволновки или мультиварки. Моющий пылесос экономит нашу энергию на махании веником и позволяет одновременно убирать пыль и мыть пол, выполняя за людей всю грязную работу. Таким образом, техника экономит кучу нашего свободного времени и сил [2].

Но что же плохого в развитии технического прогресса? И так к минусам технического прогресса можно отнести:

- Увеличение затрат на производство – с развитием технологий требуется значительно больше денег для производства продукции, так как современные технологии подразумевают использование дорогостоящего оборудования и материалов.

- Увеличение потребления энергии – развитие технологий влечет за собой увеличение потребления энергии. Это приводит к острой нехватке энергоресурсов, загрязнению окружающей среды и повышению цен на электричество.

- Ускорение ритма жизни – технический прогресс в основном направлен на повышение производительности труда, что в свою очередь ведет к ускорению ритма жизни. В свою очередь это может привести к стрессам и потере качества жизни.

- Безработица – многие виды работ, особенно низкоквалифицированные, становятся ненужными из-за автоматизации и роботизации производства, что приводит к росту безработицы и бедности.

- Угроза приватности – развитие технологий также приводит к угрозе приватности и персональных данных, так как информация может быть легко украдена или использована без соответствующего согласия.

В современном мире огромную популярность получили мобильные телефоны. Они значительно упрощают жизнь людей, но несут за собой и опасность. Угроза приватности стала частой проблемой. Если не быть аккуратными, то наши данные могут попасть в руки злоумышленников, которые в свою очередь могут совершить опасные действия или угрозы, так называемый телефонный терроризм или хулиганство.

Разберёмся сначала с тем, что такое телефонное хулиганство? Это преступное деяние, заключающееся в намеренном звонке по телефону или отправке сообщений с целью: Розыгрышей. Часто хулиганы преследуют одну цель – подшутить над жертвой. Люди представляются знакомыми собеседника, даже могут делать похожие голоса. Нередко «шутники» представляются сотрудниками государственных учреждений или банков. Конечно, розыгрыши не несут за собой каких-то серьезных проблем, но сказаться на настроении жертвы и психоэмоциональном состоянии может. Следующая

более серьёзная цель – это оскорбления и угрозы. Здесь злоумышленники оскорбляют ни в чём не виновную жертву. Желая унизить и возможно добиться ответной агрессивной реакции. Весь диалог ведётся с обилием нецензурной брани.

Такие звонки или сообщения часто могут быть анонимными, и направлены на человека, его бизнес или места общественного значения. В результате такого хулиганства часто возникают неприятности для жертвы и могут причинять ущерб физическому и эмоциональному здоровью.

Уже более серьёзные последствия за собой введёт телефонный терроризм.

Телефонный терроризм – это звонки или сообщения, в которых угрожают террористическими действиями, взрывами, нападениями или другими формами насилия. Целью телефонного терроризма может быть создание паники, проверка систем безопасности, отвлечение полиции от реальных преступлений или просто поддержание хаоса и страха.

Точно также, как и телефонное хулиганство - терроризм часто совершается анонимно, что затрудняет задержание преступников. Звонки могут идти как на уровне отдельных лиц, так и на уровне массовых звонков по городской телефонной сети или социальным сетям.

Телефонный терроризм является серьезным нарушением закона и может привести к проверкам со стороны полиции, эвакуации людей из зданий, задержанию и судебному преследованию преступника. В случае получения угрозы террористических действий необходимо немедленно связаться с правоохранительными органами и сообщить о случившемся.

Таким образом, на основании вышеизложенного можно сделать вывод, что Телефонный терроризм и телефонное хулиганство относятся к неправомерному использованию телефона для нарушения прав и интересов других лиц.

Оба вида поведения являются правонарушениями, которые могут привлечь к себе внимание правоохранительных органов и привести к уголовной ответственности.

Когда вторгаются в твою личную жизнь, нарушают твои права и создают тебе неудобства, а иногда и какие-либо серьезные проблемы такие как, например, причинение ущерба, хочется, чтобы этот злоумышленник понёс наказание за свои действия.

К сожалению, наказать нарушитель не так уж и просто. Для начала узнаем, как и что делать, если вы столкнулись с такой проблемой. В такой ситуации целесообразней обращаться в полицию, когда звонки поступали неоднократно. Потерпевший имеет право обратиться в ближайший отдел полиции и написать заявление на звонящего. Ему потребуется подробно описать все действия «пранкера», а также по возможности предоставить запись телефонного разговора.

Приняв сообщение о правонарушении, проводится проверка. В зависимости от обстоятельств дела, заявление может рассматриваться:

– трое суток по общему правилу;

– до 10 дней, если ходатайство поступило от должностного лица, проводящего соответствующую проверку;

– до 30 дней, если требуется провести дополнительные мероприятия.

Какое же наказание понесёт злоумышленник? Всё зависит от тяжести злодеянии, телефонному хулигану может грозить одно из следующих наказаний:

– Административное. Такие меры применяются по отношению к тем лицам, которые звонят гражданам. В данном случае речь не идет о нарушении общественного порядка, поскольку действия пранкера направлены на конкретного человека или лиц.

– Уголовное. Если хулиган предоставляет ложные сведения государственным органам, то в этом случае можно говорить о нарушении общественного порядка. За подобные действия предусмотрено уголовное наказание.

Важно отметить, что телефонный розыгрыш не будут считать за

правонарушение если:

– Отсутствие злого умысла. «Шутник» не преследовал цель оскорбить или запугать абонента. Речь идет о невинном розыгрыше, призванным поднять настроение не только звонившему, но и его собеседнику.

– Абоненту не был причинён какой-либо ущерб.

Административное наказание: Статья 20.1 КоАП РФ не применяется по отношению к телефонным хулиганам. Мелкое хулиганство предполагает противоправные действия в общественном месте, в то время как в телефонном разговоре участвует всего два человека [1].

Ответственность за оскорбление: Если в ходе разговора с злоумышленниками они пытались унизить или оскорбить вас и использовали при этом нецензурную брань, то в соответствии со статьей 5.61 КоАП РФ, потерпевший может привлечь правонарушителя к ответственности за оскорбление.

Человека, виновного в телефонном хулиганстве, можно наказать по части 1 вышеуказанной статьи.

Если же «пранкера» признают виновным по 5.61 КоАП РФ, он должен будет выплатить штраф в размере 3-5 тысяч рублей.

Административная ответственность за ложный вызов спецслужб

Хулиганством будет считаться ложные вызовы следующих спецслужб:

– пожарная охрана;

– скорая помощь;

– полиция;

– МЧС;

– аварийная газовая служба и т. д.

Звонок на горячую линию без уважительных причин может обернуться для звонившего административным наказанием. В соответствии со статьей 19.13 КоАП РФ, размер взыскания составит до 1500 рублей.

Ложное сообщение о терроризме: Если пранкер предоставил ложные сведения о террористическом акте, то его привлекут к ответственности по статье 207 УК РФ [4]. В отношении таких нарушителей применяют термин «телефонный террорист». Обязательными признаками таких преступлений являются:

– звонивший знает, что предоставляет ложные данные;

– хулиган сообщает о подготовке теракта, а не о совершенном преступлении;

– звонок поступает в государственные органы, которые обязаны отреагировать на подобную заявку.

Совершив подобное преступление, злоумышленник понесет одно из следующих наказаний:

– от 200 до 500 тысяч рублей штрафа;

– штраф в размере дохода злоумышленника в течение 12-18 месяцев;

– до трех лет принудительных работ;

– ограничение свободы до трех лет.

Более серьезным будет наказание, если действия информатора направлены на банки, школы, детские сады, больницы, развлекательные центры и прочие объекты инфраструктуры. В таких случаях ответственность наступает по части 2 статье 207 УК РФ. Возможны следующие меры пресечения:

– штраф в размере 500-700 тысяч рублей;

– штраф в размере дохода, осужденного за период 1-2 года;

– от трех до пяти лет лишения свободы.

Рассмотрим программное обеспечение и телефонный терроризм. Какие программы помогают злоумышленникам?

Для совершения телефонного терроризма или хулиганства злоумышленники могут использовать некоторые виды программного обеспечения, например:

– Автоматические наборщики номеров – это программы, которые автоматически набирают телефонные номера и звонят на них. Такие программы могут быть настроены на повторное набирание номера в случае, если вызов не был принят, и дозваниваться до тех пор, пока кто-то не ответит.

– Спам-боты – это программы, которые отправляют автоматические сообщения на телефоны. Они могут быть настроены на отправку сообщений с угрозами, оскорблениями или другого рода неприятностями.

– Программы, которые изменяют свой номер – это программы, которые могут изменять номер телефона отправителя звонка или сообщения. Это может создавать проблемы для правоохранительных органов, которые пытаются отследить их идентификатор.

– Программы, которые делают голосовые изменения – это программы, которые могут изменять голос злоумышленника. Это может быть использовано для того, чтобы скрыть свою личность и создать более убедительную угрозу.

– Программы-диктофоны – это программы, которые могут записывать телефонные разговоры без уведомления собеседника. Это может быть использовано для того, чтобы собирать компромат или создавать доказательства в свою пользу.

Как правило, злоумышленники используют комбинацию различных программ для совершения телефонного терроризма. Например, они могут использовать автоматические наборщики номеров и спам-боты для набивания линии и отправки сообщений с угрозами, а также программы, которые изменяют свой номер и голосовые изменения, чтобы скрыть свою личность.

Какие программы помогают от злоумышленников?

Современные телефонные системы используют различные методы защиты от телефонного терроризма. Ниже приведены наиболее распространенные методы:

– Блокировка номеров: этот метод позволяет заблокировать номера телефонов, с которых поступают нежелательные звонки. Это можно сделать вручную или автоматически с помощью программного обеспечения.

– Анализ голоса: некоторые телефонные системы используют технологию анализа голоса, чтобы определить, является ли звонок нежелательным. Этот метод основывается на идентификации характерных свойств голоса, которые указывают на то, что звонок может быть спамом.

– Фильтрация сообщений: некоторые телефонные системы позволяют фильтровать текстовые сообщения, которые могут содержать нежелательные предложения или ссылки на мошеннические сайты.

– Проверка на спам: некоторые телефонные системы проводят проверку на спам, используя базы данных с известными номерами телефонов спамеров.

– Автоматическая блокировка: некоторые телефонные системы могут автоматически блокировать звонки с номеров, которые были ранее заблокированы другими пользователями.

– Регистрация в списке не звонить: некоторые телефонные системы используют список не звонить, который содержит номера телефонов людей, которые не хотят получать нежелательные звонки.

Какие компании помогают бороться с злоумышленниками?

Существует множество компаний, которые занимаются разработкой программного обеспечения и обучением персонала для защиты от телефонного терроризма. Некоторые из них:

– «Cisco» - компания, которая предоставляет решения для защиты от кибератак, включая защиту от телефонного терроризма.

– «Avaya» - компания, специализирующаяся на технологиях связи, предлагает инструменты для защиты от телефонных атак.

– «Symantec» - компания, которая предоставляет решения для защиты от

киберугроз, включая защиту от телефонного терроризма.

– «Kaspersky Lab» - компания, специализирующаяся на разработке антивирусного программного обеспечения и решений для защиты от кибератак, включая защиту от телефонного терроризма.

– «Check Point» - компания, которая предоставляет решения для защиты сетей от киберугроз, включая защиту от телефонного терроризма.

– «SecureLogix» - компания, специализирующаяся на защите от телефонных атак и предоставляющая решения для защиты от телефонного терроризма.

– «Verint» - компания, которая предоставляет решения для защиты от киберугроз, включая защиту от телефонного терроризма, а также обучение персонала по защите от кибератак.

Способы защититься от утечки данных и телефонных террористов.

Для того чтобы обезопасить себя от телефонных террористов следует тщательно следить за своими данными, где вы регистрируетесь, по каким ссылкам переходите, на каких сайтах вы сидите. Самым надёжным средством от злоумышленников будет прежде всего наша внимательность. Способы для защиты от утечки своих данных.

– Используйте сильные пароли и не повторяйте их на разных сайтах. Регулярно меняйте пароли.

– Не отвечайте на подозрительные письма, SMS-сообщения и звонки от незнакомых людей или компаний.

– Установите антивирусное программное обеспечение на свое устройство и регулярно обновляйте его.

– Не делитесь личной информацией в социальных сетях и других онлайн-платформах.

– Не храните конфиденциальную информацию на общедоступных устройствах или в облачных хранилищах.

– Используйте VPN-сервисы для шифрования интернет-трафика и защиты своей конфиденциальности.

– Запретите нежелательным звонкам и сообщениям на вашем телефоне с помощью приложений блокировки.

– Не предоставляйте свой номер телефона или адрес электронной почты на ненадежных сайтах.

– Будьте осторожны при использовании общественных Wi-Fi-сетей и не отправляйте личную информацию через них.

– Регулярно проверяйте свои финансовые отчеты и уведомления о кредитах на наличие подозрительных операций.

– Не скачивать файлы от незнакомых отправителей.

– Использовать двухфакторную аутентификацию.

– Использовать PIN- и PUK-код.

Возможные последствия телефонного терроризма: Какие последствия может иметь телефонный терроризм для обычных людей? Телефонный терроризм может иметь серьезные последствия для обычных людей, включая:

– Потерю времени и нервов: Необходимость отвечать на звонки с угрозами или непристойными сообщениями может отнимать время и энергию, а также вызывать стресс и беспокойство.

– Психологические проблемы: Постоянное нахождение под угрозой может вызывать психологические проблемы, такие как тревога, депрессия и посттравматическое стрессовое расстройство.

– Финансовые потери: Некоторые формы телефонного терроризма могут привести к финансовым потерям, например, если злоумышленник запрашивает выкуп или угрожает повредить имущество.

– Угроза личной безопасности: в некоторых случаях телефонный терроризм

может представлять угрозу личной безопасности, особенно если злоумышленник знает ваш адрес или место работы.

– Юридические проблемы: если злоумышленник нарушает закон, например, отправляя угрозы или непристойные сообщения, это может привести к юридическим проблемам, включая арест и судебное преследование.

В целом, телефонный терроризм может серьезно повлиять на жизнь людей и вызвать различные проблемы, поэтому важно принимать меры для защиты себя и своих близких [3].

Последствия телефонного терроризма для компаний и организаций: Телефонный терроризм может иметь серьезные последствия для компаний и организаций в различных сферах, включая финансовые услуги и информационную безопасность. Во-первых, он может привести к значительным финансовым потерям. Компания может быть вынуждена закрыть свои операции на несколько дней или недель, что может привести к потере прибыли и ущербу репутации. Во-вторых, телефонный терроризм может привести к утечке конфиденциальной информации. Злоумышленник может выдавать себя за представителя компании и запрашивать у клиентов и сотрудников конфиденциальные данные, такие как пароли, номера социального страхования, номера банковских счетов и т.д. Это может привести к утечке данных, которые могут быть использованы для мошенничества и кражи личности. В-третьих, телефонный терроризм может повредить репутации компании. Если клиенты узнают о случаях телефонного терроризма, это может снизить их доверие к компании и вызвать отток клиентов.

В целом, телефонный терроризм может привести к серьезным последствиям для компаний и организаций, особенно в сфере финансовых услуг или информационной безопасности. Поэтому важно принимать меры для предотвращения таких инцидентов, например, обучать сотрудников, как правильно общаться с клиентами по телефону, проверять личность звонящего и использовать защищенные каналы связи.

В заключение следует отметить о том, что технический прогресс – это процесс, который позволяет нам создавать новые технологии, устройства и инструменты, которые улучшают нашу жизнь и способствуют развитию общества. Однако, споры о том, хорошо ли влияет технический прогресс на человечество или плохо, продолжаются. Важно найти баланс между использованием новых технологий и человеком.

Важным вопросом в теме технического прогресса является вопрос этики и правильном использовании изобретений. На просторах интернет-ресурсов можно столкнуться с множеством неприятностей, например, утечка данных, которые уже в свою очередь могут, столкнут вас с телефонными террористами или хулиганами.

Подводя итог всему вышесказанному, можно сказать, что к счастью, есть несколько способов защититься от телефонных террористов:

- во-первых, никогда не давайте свои личные данные по телефону, особенно если звонок пришел от незнакомого номера;

- во-вторых, не поддавайтесь на угрозы и требования телефонного террориста. Лучше всего сразу же завершить звонок и сообщить о случившемся полиции. Если вам все же звонил телефонный террорист, то важно запомнить время звонка, номер телефона и содержание разговора. Чтобы избежать телефонного терроризма в будущем, можно использовать специальные приложения и программы, которые блокируют нежелательные звонки и сообщения.

Перечень использованной литературы и источников:

1. Кодекс Российской Федерации об административных правонарушениях [Текст]: от 30.12.2001 № 195-ФЗ (ред. от 24.04.2020) // Собрание законодательства РФ. – 07.01.2002. – № 1 (ч. 1).

2. Шаньгин В. Ф. Информационная безопасность и защита информации / В. Ф. Шаньгин. – 2-е изд. – Саратов: Профобразование, 2019. – 702 с. [Электронный ресурс] // Цифровой образовательный ресурс IPR SMART. – URL: https://www.iprbookshop.ru/87995.html (дата обращения: 20.12.2023).

3. Основы информационной безопасности: учебник для студентов вузов, обучающихся по направлению подготовки «Правовое обеспечение национальной безопасности» / В.Ю. Рогозин, И.Б. Галушкин, В.К. Новиков, С.Б. Вепрев. – Москва: ЮНИТИ-ДАНА, 2017. – 287 с. [Электронный ресурс] // Цифровой образовательный ресурс IPR SMART. – URL: https://www.iprbookshop.ru/72444.html (дата обращения: 19.12.2023).
4. Уголовный кодекс Российской Федерации: федер. закон от 13.06.1996 № 63-ФЗ (ред. от 07.04.2020) // Собрание законодательства РФ. – 17.06.1996. – № 25.

2.5. ИСПОЛЬЗОВАНИЕ «ЭЛЕКТРОННОЙ ПОДПИСИ» КАК СПОСОБА ЗАЩИТЫ ИНФОРМАЦИИ В СЕТЯХ ПЕРЕДАЧИ ДАННЫХ ОВД РОССИИ

В представленной работе авторами рассмотрены история создания, основные виды, цель, различия и преимущества использования «электронной цифровой подписи» (ЭЦП); описаны современный метод защиты системы «электронной цифровой подписи», проведен анализ термина «электронной цифровой подписи» и разрешительно-запретительных нормативно-правовых актов действующих в Российской Федерации (РФ, Россия) по вопросу использования «электронной цифровой подписи».
Ключевые слова: информационные сети, закрытый ключ, конфиденциальность, метод защиты системы ЭЦП, сертификат ключа, шифрование, электронная цифровая подпись (ЭЦП), электронный документооборот.

USING AN ELECTRONIC SIGNATURE AS A WAY TO PROTECT INFORMATION IN RUSSIAN ATS DATA TRANSMISSION NETWORKS

In the presented work, the authors consider the history of creation, the main types, purpose, differences and advantages of using an "electronic digital signature" (EDS); describe the modern method of protecting the "electronic digital signature" system, analyze the term "electronic digital signature" and permissive regulatory legal acts in force in the Russian Federation (RF, Russia) on the issue of using an "electronic digital signature".
Keywords: information networks, private key, confidentiality, EDS system protection method, key certificate, encryption, electronic digital signature (EDS), electronic document management.

Введение. На сегодняшний день используется множество различных методов защиты от подделок личной подписи - биометрические, PIN коды и т.д. В частности, широко используются системы «электронной цифровой подписи» (ЭЦП). Современные технологии позволяют передавать данные в электронном виде, что ускоряет и упрощает процессы обмена информацией. Однако, при этом возникает проблема безопасности в информационных сетях передачи данных, поскольку они могут быть подвергнуты несанкционированному доступу и изменению. Для ее решения в сетях передачи данных Органов внутренних дел России (ОВД России) применяется ЭЦП. Она позволяет гарантировать целостность и подлинность передаваемой информации, а также устанавливать авторство отправителя. С использованием ЭЦП можно обеспечить целостность, аутентификацию и непрерывность передаваемой информации, что является особенно важным в таких системах, где требуется обеспечить сохранность доказательств и обмена информацией.

Рассмотрение проблемы. История создания ЭЦП началась в 1976 году, когда ученые Уитфилд Диффи и Мартин Хеллман разработали алгоритм шифрования, который был назван «Diffie-Hellman key exchange». Этот алгоритм позволял двум участникам общаться через небезопасный канал связи, не раскрывая при этом свои секреты.

В 1985 году Рональд Ривест, Ади Шамир и Леонард Адлеман разработали алгоритм RSA, который стал одним из самых популярных методов шифрования с открытым ключом. RSA использует математические принципы для создания пары ключей, которые могут быть использованы для шифрования и расшифровки данных.

В 1991 году был создан стандарт ЭЦП («Digital Signature Standard» (DSS), который определяет требования к алгоритмам и параметрам для создания и проверки ЭЦП. DSS был разработан Национальным институтом стандартов и технологий США (NIST) и использовал алгоритм SHA-1 для хеширования данных.

В 1993 году был создан стандарт ЭЦП, который был принят как международный стандарт в 1999 году. Этот стандарт определяет процедуру создания и проверки ЭЦП, которая позволяет доказать авторство сообщения и его целостность.

С 2000 года использование ЭЦП начало распространяться в различных отраслях, таких как банковское дело, государственные учреждения и коммерческие организации. ЭЦП стала незаменимым инструментом для обеспечения безопасной передачи информации и подтверждения авторства электронных документов.

В настоящее время существует много различных протоколов и алгоритмов для создания и проверки ЭЦП. Они используются в различных приложениях и отраслях, где требуется обеспечить безопасность и целостность электронной информации. Стандарты и регуляции по использованию ЭЦП также продолжают развиваться и совершенствоваться, чтобы обеспечивать высокую степень защиты и доверия.

Определение ЭЦП, задачи и виды. В ОВД России применение электронной подписи регулируется Федеральным законом от 06.04.2013 года № 63-ФЗ «Об электронной подписи», который устанавливает виды электронных подписей, правила признания юридической силы подписанных документов, правила выдачи и использования ЭП, а также определяет основные решения проблемы обеспечения правовых условий для использования ЭЦП в процессах обмена электронными документами, при соблюдении которых ЭЦП признается юридически равнозначной собственноручной подписи человека в документе на бумажном носителе (в таблице 1 предоставлены основные различия между цифровой и собственноручной) [2, 3, 4, 6, 7, 8].

Таблица 1 – Различия собственноручной и цифровой подписи

Собственноручная подпись	**Цифровая подпись**
Не зависит от подписываемого текста (всегда одинакова).	Зависит от подписываемого текста (практически всегда разная).
Неразрывно связана с подписывающим лицом, однозначно определяется его психофизиологическими свойствами (не может быть утеряна).	Определяется секретным ключом, принадлежащая подписывающему лицу (может быть утеряна владельцем).
Неотделима от носителя (бумажный документ), поэтому отдельно подписывается каждый экземпляр документа.	Легко отделима от документа, поэтому верна для всех его копий.
Не требует для реализации дополнительных механизмов.	Требует дополнительных механизмов, реализующих алгоритмы её вычисления и проверки.
Не требует создания поддерживающей инфраструктуры.	Требует создания доверенной инфраструктуры сертификатов открытых ключей.

Под ЭЦП понимается информация в электронном формате, предназначенную для защиты электронных документов от подделки, полученная путем шифрования и преобразования информации с помощью закрытого ключа электронной подписи и позволяющая идентифицировать владельца сертификата ключа подписи [1]. Технологии ЭЦП разнообразны и дифференцированы, представлены на рисунке 1.

Рисунок 1 – Задачи и виды ЭЦП

Шифрование делится на две самые основные схемы построения ЭЦП: симметричная и ассиметричная.

1. **Симметричная схема ЭЦП на основе алгоритмов симметричного шифрования.** Данная система предусматривает использование третьего лица арбитра, пользующегося доверием обеих сторон. Аутентификацией документа является сам факт его шифрования секретным ключом и передача его арбитру.

Преимущества:

- Стойкость симметричных схем вытекает из стойкости используемых блочных шифров.

- Стойкость шифра легко заменила другим.

Недостатки:

- Каждый бит информации подписывается отдельно.

- Сгенерированные ключи используются только один раз, так как после подписания документа, часть секретного ключа раскрывается.

2. **Асимметричная схема ЭЦП на основе алгоритмов асимметричного шифрования.** Самая распространенная и наиболее применяемая в нашей жизни. В этой системе шифрование выполняют на открытом ключе, а дешифрование – на закрытом ключе получателя, то в схемах ЭЦП подпись производят с помощью закрытого ключа, а проверку – с помощью открытого ключа пользователя, который передает сообщения

Недостатки:

- Асимметричное шифрование базируется на вычислительно сложных задачах, сложность которых строго математически не доказана.

- Криптостойкость слабая, поэтому надо увеличивать длину ключей, что подвергает переписыванию программы.

Исходя из вышеуказанного Федерального закона №63-ФЗ, основной целью является установление отношений между сторонами при использовании аналога визы и печати на бумажном носителе, а также применяются во время сделок различного типа, представлено на рисунке 3.

Электронная подпись обеспечивает безопасность электронного документооборота (ЭДО). Вот несколько способов, которыми ЭЦП обеспечивает безопасность:

1. *Аутентификация.* ЭЦП позволяет проверить подлинность и идентификацию отправителя или получателя данных. В результате получаем доказательство того, что сообщение или документ отправлены именно от лица, которое указано.

2. *Целостность данных.* ЭЦП используется для проверки, не изменялись ли данные или документы после создания подписи. Если данные были изменены, то подпись становится недействительной, что помогает выявить и предотвратить несанкционированные изменения информации.

3. *Непрерывность передачи.* ЭЦП гарантирует, что сообщение или документ не были изменены или повреждены во время передачи. При использовании ЭЦП, любые изменения или повреждения будут обнаружены, и целостность информации будет защищена.

4. *Недифференцированность.* ЭЦП позволяет сделать возможным проверку подписанного документа без необходимости предоставления оригинала. Получатель может быть уверен в том, что информация, содержащаяся в документе, не была изменена.

5. *Защита от подделки.* Создание ЭЦП требует использования уникального ключа, который является уникальным для каждого пользователя. Это предотвращает подделку или возможность создания фальшивых подписей [3, 5, 6, 8].

Благодаря этому определяется владелец сертификата и после этого устанавливается неизменность информации, которая содержится в документе. В целом, электронная подпись играет важную роль в обеспечении безопасности электронных коммуникаций и обработки информации. Она позволяет подтвердить подлинность данных и идентификацию участников, гарантировать целостность информации и предотвращать несанкционированные изменения. Это делает ЭЦП незаменимым инструментом в современных информационных системах, где безопасность и доверие являются приоритетом.

Рисунок 2 Принцип действия ЭЦП

Основным требованием, предъявляемое к этому алгоритму, является исключение возможности проверки подлинности ключа и обеспечивает конфиденциальность информации.

ЭЦП можно подписать практически любой документ, который разработан внутри учреждения и утвержденный учреждением, то есть с руководителем учреждения или человеком имеющий право подписи, например, заместитель руководителя. Он должен выкладываться в виде электронного документа, то есть ЭЦП. В ОВД с помощью ЭЦП можно подписывать различные документы и формы. Вот некоторые примеры таких документов:

1. Заявления о регистрации на месте пребывания или жительства.
2. Заявления о выдаче паспорта гражданина Российской Федерации.
3. Заявления о регистрации транспортных средств.
4. Приказы, распоряжения и документы внутреннего распорядка органов внутренних дел.
5. Протоколы об административных правонарушениях.
6. Разрешения и уведомления о проведении массовых мероприятий.
7. Разрешения на хранение и ношение оружия и боеприпасов.
8. Документы, связанные с уголовным и административным производством (постановления о возбуждении уголовного дела, протоколы допроса, решения суда и т.д.).

Важно отметить, что перечень документов, которые можно подписывать ЭЦП в ОВД, может различаться в зависимости от конкретного региона и политики ОВД.

Поэтому перед использованием ЭЦП рекомендуется обратиться в соответствующий ОВД для уточнения возможности подписания конкретного документа.

Заключение. Исследование электронных документов, как объекта правоотношений, особенно в деятельности ОВД, представляется актуальным и имеет большое значение на современном этапе, исходя из определенных оснований:

1. Информация в электронно-цифровом формате на порядок мобильнее и компактнее информации на любом другом носителе;

2. Отсутствует полноценная законодательная закрепленная нормативная база, охватывающая всю сферу электронной информации;

3. Нормативное регулирование электронного документа в информационной сфере быстро развивается – особенно на ведомственном уровне;

4. Современные системы электронного обмена позволяют систематизировать учет и хранение документов, обеспечить оперативный доступ к отчетной информации, организовать управление процессами движения и обработки документов.

Таким образом, применение ЭЦП в сетях передачи данных ОВД имеет большое значение для обеспечения информационной безопасности. ЭЦП позволяет гарантировать аутентификацию отправителя и целостность передаваемых данных, что является ключевыми аспектами в правоохранительной деятельности.

Одним из главных преимуществ применения ЭЦП в сетях передачи данных ОВД является возможность проверки авторства и целостности электронных документов. Это позволяет исключить возможность подделки и прежде всего несанкционированного доступа к информации, что имеет критическое значение в правоохранительной сфере.

Применение ЭЦП также обеспечивает конфиденциальность данных, поскольку только авторизованные пользователи могут проверить их подлинность. Это позволяет органам правопорядка управлять обработкой и передачей информации, минимизируя риски утечки и несанкционированного доступа к конфиденциальным данным.

Однако, применение электронной подписи в сетях передачи данных ОВД также сопряжено с некоторыми вызовами и техническими сложностями. Необходимость обеспечения защиты и безопасности инфраструктуры передачи данных, а также обучение персонала и внедрение соответствующих стандартов являются ключевыми факторами успешной реализации ЭЦП.

В целом, применение ЭЦП в сетях передачи данных ОВД является полезным и эффективным инструментом для улучшения безопасности и целостности информации. ЭЦП позволяет сократить риски подделки и несанкционированного доступа, обеспечивает доверие к передаваемым данным и обеспечивает контроль и управление информацией в правоохранительной сфере. Дальнейшее развитие и стандартизация применения ЭЦП в ОВД будут играть важную роль в поддержании безопасности и эффективности правоохранительных операций.

Перечень использованной литературы и источников:

1. Российская Федерация. Законы. Об электронной подписи: федер. закон от 6 апреля 2011 г. №63-ФЗ (ред. От 28.06.2014) // СЗ РФ. – 2011. – №15. – Ст. 2036.

2. Гончаров Е.И., Шатковская Т.В. Проблемы применения цифровой подписи в электронном документообороте России / Е.И. Гончаров, Т.В. Шатковская // Северо-Кавказский юридический вестник. – 2020. - № 2. – С. 97-103.

3. Мещерякова Т.В. Основы применения специальной техники и информатики в профессиональной деятельности сотрудника полиции: учебное пособие / Т.В. Мещерякова, С.А. Гречаный и др. – Москва: ДГСК МВД России, 2017. – 192 с.

4. Мирошниченко А.А. Кулагин И.Н. Сравнительный анализ цифровой и электронной подписи [Электронный ресурс] / А.А. Мирошниченко, И.Н. Кулагин. – URL: https://www.tsutmb.ru/nauka/internet-konferencii/2019/aktualnye_problemy/5/Miroshnichenko_Kulagin.pdf

5. Халиков Р.О. Правовой режим электронного документа: вопросы использования электронной цифровой подписи: автореф. дис. …канд. юрид. наук: 12.00.03 / Р.О. Халиков. – Казань: ГОУ ВП «Казанский государственный университет имен В.И. Ульянова-Ленина», 2006. - 32с.

6. Черемушкин А.В. Криптографические протоколы. Основные свойства и уязвимости: учеб. пособие для студ. учреждений высш. проф. образования/ А.В. Черемушкин. – Москва: ИЦ «Академия», 2009. – 272 с.

7. Щука И.О., Нестеренко И.С., Нестеренко Г.А. Перспективы, достоинства и недостатки электронной подписи/ И.О. Щука, И.С. Нестеренко, Г.А. Нестеренко [Электронный ресурс] // Международный научно-исследовательский журнал. – 2023. - № 2 (128). – URL: https://research-journal.org/archive/2-128-2023-february/10.23670/IRJ.2023.128.7.
8. Ясенев В.Н. Конспект лекций по информационной безопасности: Конспект лекций / В.Н. Ясенев. – Нижний Новгород НИИПМК «ННГУим. Н.И. Лобачевского», 2017. – 254 с.

2.6. СОВРЕМЕННЫЕ ТЕНДЕНЦИИ РАЗВИТИЯ ИНФОРМАЦИОННЫХ ТЕХНОЛОГИЙ ПО ВЫЯВЛЕНИЮ И ПРЕДОТВРАЩЕНИЮ ПРЕСТУПЛЕНИЙ

В условиях современного информационного общества возрастает важность информационно-аналитического обеспечения планирования предупреждения преступности на региональном и муниципальном уровнях путем активного внедрения коммуникационных технологий в криминологическую деятельность.
Ключевые слова: информационно-коммуникационные технологии (ИКТ), криминологическую деятельность, правоохранительные органы, предупреждение преступлений, противодействие преступлениям, цифровизация в криминологии.

CURRENT TRENDS IN THE DEVELOPMENT OF INFORMATION TECHNOLOGIES FOR THE DETECTION AND PREVENTION OF CRIMES

In the conditions of the modern information society, the importance of information and analytical support for crime prevention planning at the regional and municipal levels is increasing through the active introduction of communication technologies into criminological activities.
Keywords: information and communication technologies (ICT), criminological activities, law enforcement agencies, crime prevention, combating crimes, digitalization in criminology.

Современные информационно-коммуникационные технологии (ИКТ) используются правоохранительными органами для противодействия преступлениям и их предупреждению. Эволюция информационных технологий используется и преступниками, они также находят новые способы совершения преступлений, связанных с такими объектами, как: интернет- торговля незаконными товарами, создание в компьютерных сетях противоправных организаций (сект и/или групп), кибератаки на финансовые системы и государственное управление, кибермошенничество и другие формы киберпреступности. Киберпреступность остается одной из серьезных проблем для большинства стран мира, а также является угрозой национальной безопасности любого государства, в т.ч., для России.

В юридической науке, противодействие преступности – это выявление, предотвращение преступных действий, а также определение причин преступлений и их устранение, проводимая государственными органами исполнительной власти [15]. Сама деятельность государственной исполнительной власти по противодействию преступности является многоуровневой, направленной, в том числе, на борьбу с новыми рисками, прогнозирование показателей преступности и предупреждение преступлений. При этом, под прогнозированием преступности, прежде всего понимается, прогнозирование ее новых форм и пути предупреждения, как известных видов преступлений, так и новых, обобщая мировой опыт и внутренние социально-экономические процессы в обществе.

Деятельность государственных органов власти в целом, и особенно правоохранительных органов по противодействию преступности, в современных условиях связана с использованием информационных технологий. Но. использование преступниками современных информационных технологий при совершении преступлений, сравнительно недавняя форма в криминологической науке, и относительно мало изученная в части методов противодействия и предупреждения таких преступлений. Изучение форм и методов борьбы с киберпреступностью – это относительно новое направление в криминологической науке.

Главенствующую роль в борьбе с преступностью имеют криминологические и уголовно-правовые основы [15]. Тем не менее инструменты информационных технологий и методы цифровизации в криминологии развиваются достаточно успешно. Авторами был проведен анализ динамики раскрываемости преступлений на федеральном и региональном уровне (на примере Хабаровского края) для изучения связи с внедрением цифровизации и информационных технологий в деятельность правоохранительных органов.

Изучая вопрос противодействия преступности (в целом) по России, были проанализированы статистические данные портала правовой статистики Генеральной прокуратуры РФ, которые демонстрируют спад количества зарегистрированных преступлений в период с 2010 по 2022 гг. [9], наблюдается постепенное уменьшение количества преступлений, что свидетельствует, в целом, о положительной динамике.

При этом, в общем значении количество зарегистрированных преступлений в год остается высоким – около 200 тыс. [10]. Динамика числа нераскрытых преступлений за аналогичный период текущего года также снижается, что в целом отражает положительную динамику и косвенно указывает на эффективность работы правоохранительных органов по борьбе с преступностью [10].

Снижение количества нераскрытых преступлений, по данным статистики МВД и Прокуратуры РФ, отражает общую положительную динамику. Но, если анализировать относительные значения раскрываемости преступлений в 2010 и в 2022 гг., то ситуация с нераскрытыми преступлениями имеет формальную положительную динамику. Так, в 2010 году зарегистрировано 2628799, а нераскрыто 1193293, где процент нераскрытых преступлений составляет 45,39% от общего числа зарегистрированных. В 2022 году зарегистрировано 1966795, а нераскрыто 904509, что составляет 45,99%. Таким образом, мы можем наблюдать, что количество нераскрытых преступлений в процентном соотношении с общим числом зарегистрированных преступлений остается неизменной. Действительную положительную динамику можно наблюдать в количестве зарегистрированных преступлений за год.

Изучая сведения по региональной статистике, отметим, что в период с 2010 по 2022 год в Хабаровском крае было зарегистрировано и нераскрыто следующее количество преступлений (См. Рис. 1) [9].

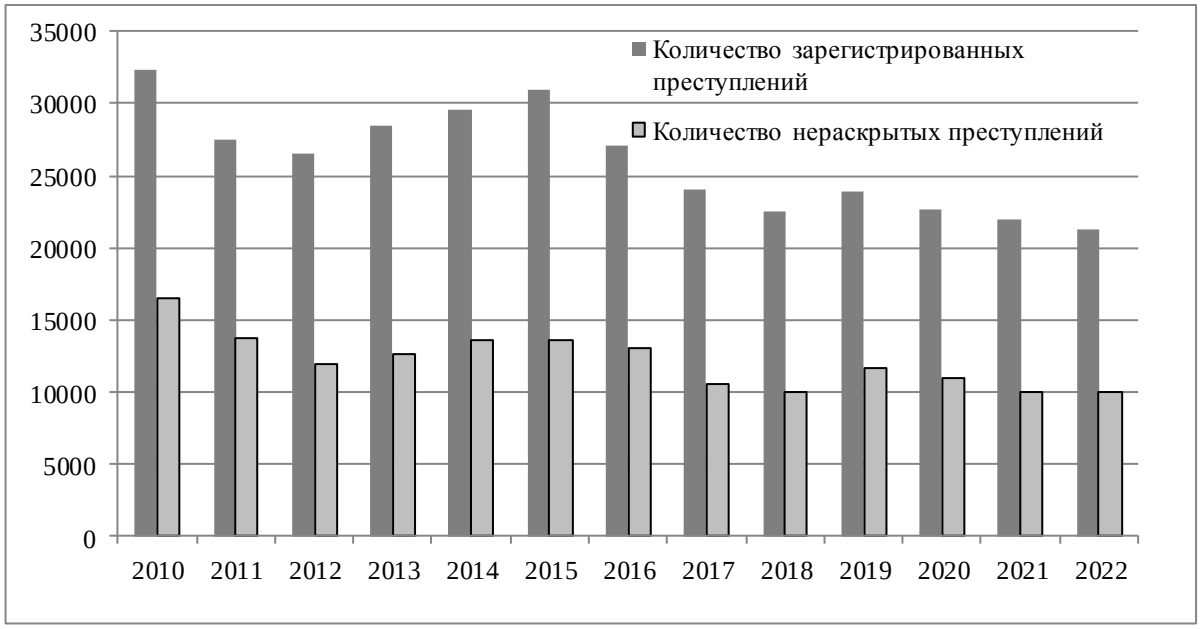


Рисунок 1 – Соотношение количества зарегистрированных и нераскрытых преступлений по Хабаровскому краю за период 2010-2022 гг. [9]

Таблица 1 – Количество зарегистрированных и нераскрытых преступлений в абсолютных значениях по Хабаровскому краю за период 2010-2022 гг. [9]

Год	Зарегистрировано преступлений	Нераскрыто преступлений
2010	32321	16449
2011	27492	13786
2012	26534	11963
2013	28465	12668
2014	29598	13569
2015	30946	13576
2016	27008	13098
2017	24043	10562
2018	22509	9956
2019	23940	11644
2020	22695	10962
2021	21987	10039
2022	21312	9959

Аналогично проанализировали количество нераскрытых преступлений в отчетном периоде в процентном соотношении к количеству зарегистрированных преступлений, получили 50,89% нераскрытых преступлений в 2010 году (самые высокие показатели преступности) и 46,72% в 2022 году. Ситуация с раскрываемостью преступлений в Хабаровском крае за 2010 по 2022 год показывает положительную динамику на 4,17%. Полагаем, что за десять лет, данный показатель мог бы быть более результативным. Возможно, причины медленных изменений в раскрываемости преступлений скрыты в используемых методах и инструментах, при выявлении и раскрытии преступлений.

На федеральном и региональном уровне темпы раскрываемости преступлений примерно такие же, как в Хабаровском крае. Отметим, что такое обобщение некорректно, ввиду соотношения численности населения, например, в Хабаровском крае и Московской области (в западной части страны численность постоянного населения на порядок выше, чем в регионах Дальнего Востока). Т.е., внутренние миграционные процессы в западных регионах России более динамичны, следовательно, и возрастает уровень преступности, если его сравнивать с Хабаровским краем, или любым дальневосточным регионом. Необходимо учитывать и нагрузку, возрастающую на органы правопорядка в части интенсивности их работы по предупреждению преступлений и раскрытию уже совершенных преступлений. На этом фоне увеличение числа раскрытых преступлений можно оценивать, как положительный индикатор работы правоохранительных органов.

Можно выделить положительную динамику уменьшения количества зарегистрированных преступлений, что также может является показателем, который отражает работу правоохранительных органов в области предупреждения и профилактики преступлений. Вопросы исследования практики предотвращения и профилактики преступлений всегда актуальны, но важно исследовать и инструменты, и методы борьбы в сфере киберпреступности и преступлений с применением средств информационных технологий.

Отдельными исследователями, например, Андреем Сергеевичем Лаптевым отмечается, что в рамках начавшейся в 2019 году реализации национального проекта «Цифровая экономика» включающего федеральный проект «Цифровое государственное управление», ориентированный на использование цифровых технологий и платформенных решений в государственном управлении, а тот в свою очередь проект «Цифровое стратпланирование», было бы целесообразно внедрять цифровые технологии в криминологическое планирование [1].

Современные методики и подходы к планированию мероприятий по борьбе с преступностью на региональном уровне не всегда соответствуют требованиям времени.

Анализ практики показывает, что криминологическое планирование часто проводится формально, без системного анализа криминогенной обстановки и прогнозов преступности. Координация между различными субъектами профилактики преступлений также недостаточна, что подтверждается исследованиями Р.М. Абызова [1] и А.В. Евсеева [2, 3].

Научное сообщество активно обсуждает необходимость автоматизации информационной работы при составлении прогнозов развития криминологической ситуации, более того, предлагаются современные инструменты прогнозирования, например, эконометрический анализ и нейросетевое прогнозирование. По мнению Т.А. Раскиной [13] и П.А. Пименова [8] прогноз криминогенной обстановки зависит от доступных ресурсов и обработки, хранения и использования значимой и достоверной криминологической информации. Статистический анализ также рассматривает методологию отбора значимой и достоверной информации в криминогенном анализе и правовой статистике.

Создание эффективной системы регионального криминологического планирования, предполагает разработку и внедрение портала «Криминологическое планирование». Криминологическое планирование стратегически и тактически важно в предотвращении преступности. Оно включает определение целей, задач и способов их достижения, что помогает обеспечить достижение поставленных целей. Самое главное, «криминологическое планирование» направлено на выстраивание системы мероприятий по противодействию и предотвращению преступлений, т. е. направлено на разработку и активное использование необходимых системных инструментов.

Предлагаемый же портал не сводится к отдельным этапам криминологического планирования (прогнозирование, мониторинг), а охватывает все его основные стадии планирования со значительным сокращением временных затрат от получения данных для окончательной реализации определенных мероприятий [7].

Зарубежный опыт использования информационных систем для анализа, прогнозирования преступности и определения мер предупреждения активно используется на протяжении последних десятилетий. Эти системы включают анализ данных из интернета и социальных сетей, а также оценку последствий проведения мероприятий. При этом опыт использования информационных систем в деятельности правоохранительных органов для осуществления анализа, прогнозирования (преступлений, личностей правонарушителей, жертв преступлений), определения мероприятий по предупреждению преступности, в том числе с привязкой к их географическому положению, оперативный анализ данных из сети Интернета, а также на основе данных из социальных сетей с дачей оценки последствий их проведения на протяжении последних десятилетий активно используется в зарубежных странах [2, 4, 18].

Принимая во внимание указанные факты, приходим к выводу, что против киберпреступности необходимо бороться передовыми средствами, а конкретно – внедрять цифровые технологии, прежде всего, технологию «Data Mining», в качестве мер борьбы и предупреждения киберпреступности. Применение методов предотвращения киберпреступности используется в зарубежной и отечественной практике с конца XX века. Такие системы на рубеже XX и XXI века уже использовались Интерполом. Сейчас в мире разрабатываются программы для решения проблем с преступностью в целом, и в частности, с киберпреступностью. Возникло новое направление - цифровая криминология.

Помимо всего перечисленного, данное направление было также отмечено в проекте Киотской декларации «Активизация мер предупреждения преступности, уголовного правосудия и обеспечения верховенства права: навстречу осуществлению Повестки дня в области устойчивого развития на период до 2030 года», где были отмечены транснациональный, организованный и сложный характер преступности, а

также использование преступниками для осуществления своей незаконной деятельности новых технологий, включая интернет, что осложняет предупреждение существующих преступлений, а также новых и зарождающихся форм преступности и борьбу с ними [13].

Современные программы для предотвращения преступности, выявлению преступлений и других форм работы правоохранительных органов: автоматизированные дактилоскопические информационные системы, система межведомственного электронного взаимодействия – служебную информационную систему, предназначенную для организации доступа электронных сервисов МВД России в систему межведомственного электронного взаимодействия, федеральная государственная информационная система «Интегрированный банк данных федерального уровня» и другие.

В этой связи, стоит привести мнение ученого Семена Яковлевича Лебедева, который пишет, что учитывая всеобъемлющую информационно-технологическую перспективу развития государственного контрольного ресурса в системе социального управления, весь социально-правовой контроль над преступностью, безусловно, должен предопределяться и сопровождаться, в первую очередь, адекватным объективным, суть - цифровым - уголовно-правовым реагированием на инновационные криминогенные и криминальные проявления, представляющим базовую правовую основу для системного обеспечения криминологической безопасности, в том числе, и в киберпространстве.

Воплощение такой идеи предполагает первостепенное решение следующих научно-практических задач:

1. Формирования, развития и реализации концепции взаимосвязей, взаимозависимостей и взаимодействий международного, правового, правоприменительного, криминологического, информационно-технологического, научно-практического и прочих ресурсов, направленных на обеспечение состояния защищенности личности, общества и государства от посягательств, культивируемых, прежде всего, в киберпространстве с помощью информационных технологий.

2. Оптимизации посредством криминологического и информационно-технологического потенциалов инновационного уголовно-правового ресурса как правовой основы криминологической кибербезопасности, причем, охватывающей полем своего правового контроля не только инновационную преступность в киберпространстве, но и традиционную преступность, культивируемую в обычной (не виртуальной) социальной среде, однако так или иначе связанную с цифровыми технологиями.

3. Формирование цифрового ресурса для обнаружения и регистрации правонарушений с использованием видеокамер, мобильных устройств с искусственным интеллектом, дронов с видеокамерами и функцией распознавания лиц, которые могут не только передавать изображение в реальном времени, но и преследовать и идентифицировать преступников.

4. Формирования инновационной системы выявления, пресечения и раскрытия преступлений с использованием в оперативно-розыскной деятельности современных цифровых криминалистических средств (форензики), специальных цифровых инструментов негласного получения оперативно-розыскной информации.

5. Формирования инновационной системы предварительного расследования преступлений с применением оцифрованного уголовно-правового ресурса, приобщением к уголовным делам актуальных данных с цифровой диагностической карты, установлением всех объективных обстоятельств по уголовному делу, включая свойства и качества личности обвиняемого.

6. Формирования инновационной системы объективной квалификации и оценки уголовно наказуемых деяний в приговорах с использованием оцифрованного уголовно-

правового ресурса, персональных социально-криминологических данных правонарушителей, цифровой системы определения оптимальной меры наказания - «электронные весы правосудия», технологий «блок-чейн» в уголовном процессе, иных инновационных технологий в сфере уголовного судопроизводства.

7. Формирования инновационной системы контроля над осужденными во время отбывания ими наказания, при условно-досрочном освобождении, в период судимости, в том числе, в рамках административного надзора с применением видеокамер с функцией распознавания лиц, инновационных средств дистанционного контроля над преступностью.

8. Формирования, развития и постоянной поддержки разнообразных информационных социально-правовых взаимосвязей, взаимозависимостей и взаимодействий на международном и национальном, государственном, общественном и личностном, правовом и правоприменительном, кадровом и образовательном, а также, иных уровнях, способных обеспечивать охрану общественных отношений, а также «на дальних подступах» предвидящих и прогнозирующих криминологические риски и угрозы, в результате чего будет достигнут достаточно высокий уровень предупреждения как инновационной, так и традиционной преступности.

В качестве вывода отметим следующее. Положительная динамика в уменьшении количества преступлений не превалирует над количеством нераскрытых преступлений, так как фактически, с 2010 по 2022 год, показатели нераскрытых преступлений в процентном соотношении остались неизменными, изменилось их количество, следовательно, необходимы новые качественные подходы работы правоохранительных органов. В «новых качественных подходах работы правоохранительных органов», мы видим принципиально новые инструменты и средства цифровизации и информационно-технологические системы.

В российской системе правоохранительных органов, как на федеральном, так и на региональных уровнях, активно внедряются и применяются современные информационно-цифровые технологии, и на сегодняшний день, тенденция цифровизации не спадает. Преступность трансформируется, появляются новые способы совершения преступлений с использованием современных технологий, что невольно вызывает необходимость технологического совершенствования правоохранительных органов в РФ, и работа в этом направлении ведется достаточно успешно.

Перечень использованной литературы и источников:

1. Абызов Р.М. Региональная криминология: учебник / Р.М. Абызов. – Барнаул: Федеральное государственное казенное образовательное учреждение высшего профессионального образования «Барнаульский юридический институт МВД России», 2021. – 416 с.

2. Евсеев А.В. Зарубежный опыт организации криминологического обеспечения деятельности правоохранительных органов / А.В. Евсеев // Вестник Всероссийского института повышения квалификации сотрудников Министерства внутренних дел Российской Федерации. – 2020. – № 2(54). – С. 90-97.

3. Евсеев А.В. Организация криминологического обеспечения деятельности органов внутренних дел на районном уровне: автореф. дис. ... канд. юрид. наук: 12.00.11, 12.00.08 / Андрей Васильевич Евсеев. – Москва: Моск. ун-т МВД РФ, 2016. – 31 с.

4. Институт штатных криминологов (криминальных аналитиков): зарубежный опыт и перспективы внедрения в систему профилактики правонарушений в Российской Федерации / А.Н. Варыгин, Е.В. Червонных, А.С. Клементьев, П.А. Пименов // Всероссийский криминологический журнал. – 2019. - Т. 13, № 3. – С. 506-518.

5. Кубасов И.А., Стрельников Ф.И. К вопросу решения проблем повышения производительности информационных систем на примере центрального комплекса ЦИАДИС МВД России / И.А. Кубасов, Ф.И. Стрельников // Вестник Воронежского института ФСИН России. – 2018. - № 4. – С. 67-73.

6. Кубасов И.А. Вопросы повышения эффективности использования автоматизированных дактилоскопических учетов при раскрытии и расследовании преступлений / И.А. Кубасов, Ф.И. Стрельников, Ю.С. Лунев // Вестник Воронежского института МВД России. – 2020. - № 2. – С. 231-236.

7. Новикова О.Ю. Методы и алгоритмы поддержки принятия решений центрами оперативно-разыскной информации: дис. ... канд. тех. наук: 05.13.10 / О.Ю. Новикова. – Москва: АУ. МВД РФ, 2015. – 28с.

8. Пименов П.А. Современные средства и методы криминологического прогнозирования: отечественный и зарубежный опыт: аналитический обзор / П.А. Пименов. – Москва: АУ МВД России, 2014. – С. 24-25.
9. Показатели преступности в Российской Федерации за 2010-2022 гг.: Официальный интернет-портал Генеральной прокуратуры Российской Федерации. – URL: https://epp.genproc.gov.ru/web/gprf/activity/crimestat (дата обращения 15.10.2023).
10. Показатели преступности в Российской Федерации за 2010-2022 гг.: Официальный интернет-портал МВД Российской Федерации. – URL: https://мвд.рф/reports (дата обращения 15.10.2023)
11. Проект Киотской декларации «Активизация мер предупреждения преступности, уголовного правосудия и обеспечения верховенства права: навстречу осуществлению Повестки дня в области устойчивого развития на период до 2030 года». – URL: https://www.unodc.org/ (Дата обращения 25.10.2023).
12. Прозрачный блокчейн: TADVISER. Государство. Бизнес. Технологии. – URL: https://www.tadviser.ru/index.php/Продукт:Прозрачный_ блокчейн#cite_note-3 (Дата обращения 15.11.2023).
13. Раскина Т.А. Теоретические аспекты аналитической деятельности прокуроров по профилактике преступности и правонарушаемости / Т.А. Раскина // Криминологический журнал Байкальского государственного университета экономики и права. – 2016. Т. 10, № 1. – С. 170-178.
14. Суходолов А.П. Цифровая экономика: электронный мониторинг правонарушителей и оценка его экономической эффективности / А.П. Суходолов, Б.А. Спасенников, Б.А. Швырев // Всероссийский криминологический журнал. – 2017. – Т. 11, № 3. – С. 495-502.
15. Уварова Е.С. Совершенствование уголовно-правовых и криминологических основ противодействия преступлениям, совершенным с использованием информационных, коммуникационных технологий / Е.С. Уварова, В.М. Смирнов // Молодой ученый. – 2023. - № 30 (477). – С. 108-110.
16. Big data как современный криминологический метод изучения и измерения организованной преступности / А.П. Суходолов, С.В. Иванцов, Т.В. Молчанова, Б. А. Спасенников // Всероссийский криминологический журнал. – 2019. – Т. 13, № 5. – С. 718-726.
17. Sukhodolov A.P. Artificial Intelligence in Crime Counteraction, Prediction, Prevention and Evolution / A.P. Sukhodolov, A.M. Bychkova // Russian Journal of Criminology. – 2018. – Vol. 12, No. 6. – P. 753-766.
18. The Los Angeles Police Department Is Predicting and Fighting Crime With Big Data. – URL: https://datafloq.com/read/los-angeles-police-department-predicts-fights-crim/ (Дата обращения: 10.11.2023).

2.7. ОСНОВНЫЕ НАПРАВЛЕНИЯ ИНФОРМАЦИОННОЙ БЕЗОПАСНОСТИ В УСЛОВИЯХ ЦИФРОВИЗАЦИИ

В условиях современного уровня развития информационных технологий и систем, которые позволяют применять новые способы передачи, хранения, обработки информации, актуальным вопросом является обеспечение информационной безопасности. Несанкционированное использование информации может принести значительный ущерб производственно-хозяйственным организациям и государству в целом. В статье рассматриваются понятия безопасность, информационная безопасность. Информационная безопасность является важной составляющей национальной безопасности. Определены угрозы информационной безопасности в условиях цифровизации. Сформулированы основные направления по обеспечению информационной безопасности на современном этапе экономического развития.
Ключевые слова: безопасность, информационная безопасность (ИБ), информационные системы (ИС), информационные технологии (ИТ), информация, национальная безопасность, цифровизация.

THE MAIN DIRECTIONS OF INFORMATION SECURITY IN THE CONDITIONS OF DIGITALIZATION

In the conditions of the current level of development of information technologies and systems that allow the use of new methods of transmission, storage, processing of information, an urgent issue is ensuring information security. Unauthorized use of information can cause significant damage to industrial and economic organizations and the state as a whole. The article discusses the concepts of security, information security. Information security is an important component of national security. Threats to information security in the conditions of digitalization have been identified. The main directions for ensuring information security at the present stage of economic development are formulated.
Keywords: security, information security (IS), information systems (IS), information technology (IT), information, national security, digitalization.

Информационная безопасность (ИБ) представляет собой глобальную проблему, характерную для современного этапа исторического развития. Применение новейших средств передачи, обработки и хранения информации влекут за собой возникновение сложностей в этой сфере, так как направлены на масштабное применение автоматизированных систем.

В нынешний век информатизации общества человечество вынуждено обращать серьезное внимание на проблемы информационной безопасности. Поскольку все виды деятельности в обществе и государстве тесным образом взаимосвязаны и направлены на использование большого объема информации.

В современном мире информацию уже невозможно назвать простым вспомогательным ресурсом для осуществления производственной или хозяйственной деятельности. Информация как стратегический ресурс обладает определенной стоимостью, которая может принести ее пользователю определенный уровень дохода, либо, наоборот, убыток, связанный с низким качеством информации или ее несвоевременностью.

Это порождает проблемы, связанные с возникновением индустрии получения и переработки информации. Внедрение современных информационных систем позволяет широкому кругу пользователей и производственных организаций свободно обращаться с информацией. Доступность и большая скорость получения информации, и огромное количество данных способствуют возникновению угроз безопасности используемых данных.

Информационные технологии (ИТ) на современном этапе существенным образом повлияли на все сферы жизнедеятельности общества и государства. Увеличение темпов научно-технического прогресса, скоростной режим распространения информации, не в полной мере отработанные механизмы контроля над данными процессами ведут к определенным угрозам в области информационной безопасности.

Крупномасштабное развитие информационных систем (ИС) и ИТ способствовало изменению качественных возможностей интеллекта человека, что, в свою очередь, привело к использованию огромных массивов информации и сокращению значительного числа мелких и трудоемких операций. Такие активные изменения послужили основой для объединения государств в единый пространственный базис и глобальным преобразованиям в экономике. В этой ситуации, так или иначе, начинает действовать сетевой принцип, который ведет к перестройке общества, основанной на применении современных ИТ.

Это, в свою очередь, имеет положительные моменты, а именно, дает возможность использовать большое количество информационных и интеллектуальных ресурсов. В то же время, несмотря на крупномасштабность таких процессов, они оказывают и негативное воздействие на качественные характеристики информации и ее структуру, а также ограничивают независимость государства.

В результате использования по всему миру ИС и ИТ во всех сферах жизнедеятельности человека появилась совершенно новая цифровая эпоха. Характерной ее особенностью является цифровое распространение, обработка и хранение информации, иными словами, наглядно наблюдаются процессы трансформации информационного ресурса.

Следует подчеркнуть, что цифровизация оказывает влияние на различные уровни государственного устройства, предприятий и организаций. К примеру, процессы производства в промышленности находятся под полным контролем автоматизированных систем.

Современный бизнес функционирует с использованием современных ИТ, физические лица активно сосуществуют с социальными и инженерными сетями.

Следует отметить, что в современных экономических условиях стабильно увеличивается скорость обмена информацией в сетях, и все субъекты, которые участвуют в цифровом процессе, так или иначе, заинтересованы в том, чтобы политическая, экономическая, производственная информация была доступна для заинтересованных лиц, но вместе с тем, есть и другая, не менее важная составляющая цифровизации – защита информации.

Термин «безопасность» включает в себя обширные интересы, как на уровне государства, так и на уровне личности [4, с.56]. Человечество с древних времен было заинтересовано в защите конфиденциальной информации от модификации, кражи, ознакомления.

Независимость и стабильность деятельности хозяйствующих субъектов могут быть нарушены в связи с несоблюдением технологии обработки информации, разглашением, фальсификацией, уничтожением или неправомерным использованием информации. Такие процедуры при применении развивающихся ИТ в условиях цифровизации могут нанести ущерб как в материальном, так и в моральном плане. Поэтому на данном этапе экономического развития актуальным является обеспечение ИБ.

Особую значимость проблемы ИБ обретают в нынешних условиях, когда обычные процессы по сохранению информации переходят совершенно новую техническую сферу.

Далее в рамках данной статьи важно рассмотреть, что представляет собой ИС. В целом, информационная система, как составляющая информационных технологий, это система техническая и организационная, которая выполняет соответствующие операции по предоставлению информационных технологий и информации, позволяющие удовлетворять потребности пользователей различных сфер, направленных на создание и использование информационных ресурсов [4, с.172].

Опираясь на положения Федерального закона Российской Федерации от 27 июля 2006 года № 149-ФЗ «Об информации, информационных технологиях и защите информации», информационная система – это организованный набор документов или серия документов и информационных технологий, в том числе использование информационных технологий и коммуникаций, реализующих информационные процессы [3, Ст. 2].

Созданный и используемый уровень защиты ИС дает возможность обеспечить сохранность данных, противодействовать всевозможным угрозам и атакам, исключать несанкционированный доступ. Но вместе с тем весьма проблематично считать используемую сеть неуязвимой и универсальной с точки зрения защиты информации. Возможны ситуации, когда ИС не обеспечивает должной защиты и устройства подвергаются внешнему проникновению.

Важной задачей при рассмотрении основных направлений ИБ в условиях цифровизации представляется обобщение понятия «информационная безопасность». Таким образом, можно сказать, что ИБ направлена на использование и применение необходимых методов защиты информации и ее инфраструктуры от различных видов воздействия.

Надо подчеркнуть, что ИБ является важной составляющей национальной безопасности. Один из основных гражданско-правовых документов в области стратегического планирования «О стратегии национальной безопасности в Российской Федерации» содержит важнейшие составляющие национальной безопасности [1, статья 111]. В соответствии с этим документом национальная безопасность включает в себя экономическую, экологическую, транспортную, общественную, энергетическую и информационную безопасность.

Стратегия национальной безопасности Российской Федерации направлена на обеспечение защиты национальных интересов РФ и включает реализацию

национальных интересов в области сохранения человеческого капитала, обороны страны, поддержания и развития общественной и государственной безопасности, а также информационной безопасности.

В документе подчёркивается, что угрозы ИБ неизбежны в связи со стремительным развитием коммуникационных и информационных технологий, а также усиливается воздействие на информационные ресурсы Российской Федерации со стороны иностранных государств.

Следует подчеркнуть, что ИБ, как составляющая национальной безопасности, базируется на конкретных принципах, которые в дальнейшем будут рассмотрены. Так, один из принципов основывается на сохранении первоначальной структуры информации посредством передачи, обработки и ее хранении, иными словами, внесение изменений и преобразование информации возможно осуществить только при наличии соответствующего доступа.

Следующий принцип, который лежит в основе ИБ, направлен на использование информации ограниченным кругом лиц, которые включены в информационную систему и полностью идентифицированы.

Еще один из принципов ИБ, который также нельзя оставить без внимания, предполагает, что информация должна предоставляться без ограничений пользователям, которые имеют на это соответствующие права.

Повсеместное внедрение и использование цифровых технологий в различных отраслях и сферах деятельности человека, ведет в целом к увеличению масштабов таких систем и усложнению процессов по поддержанию их в режиме функционирования, соответствующего его техническим характеристикам и параметрам.

Важное значение в рамках данного направления исследования представляет рассмотрение угроз в сфере ИБ. Современный этап развития общества и государства в условиях цифровизации экономики характеризуется значительным числом угроз, противоборство с которыми представляет собой одно из главных направлений деятельности государства в составе национальной безопасности.

Тем не менее, применение современных ИТ создает благоприятную основу для нарушителей, которые изобретают новейшие способы и методы, позволяющие нанести ущерб информационной безопасности. В компетенцию государственных органов входит задача по нейтрализации таких угроз в сфере информационной безопасности с использованием цифровых технологий и подготовку мероприятий, направленных на повышение качества борьбы с такими угрозами.

Осуществление переустройства производственного и общественного в нынешних условиях, так или иначе, должно основываться на применении и использовании достижений в сфере цифровизации.

Очевидно, что применение современных ИС и ИТ в условиях постоянно совершенствующейся цифровизации неуклонно ведет к возникновению различного рода угроз. Иными словами, основные проблемы, возникающие в сфере информационной безопасности, с которыми сталкивается цифровизация, так или иначе направлены на подрыв национальной безопасности государства [7, с.123].

Угрозу ИБ для нашего государства представляет деятельность специальных подразделений международных организаций и дезинформация населения о совершаемых террористических атаках в сети «Интернет», призывы к проведению несанкционированных собраний и митингов.

В качестве примера в области ИБ и ее защиты можно рассмотреть проведение СВО на Украине. Данная ситуация дала новый импульс к изменению информационной ситуации и информационной безопасности в стране.

Для обеспечения национальной безопасности и защиты суверенитета страны необходимо провести колоссальную работу. «Коллективный Запад» во главе США,

развязавший информационную войну против России, заставляет наше государство разрабатывать и применять все новые и новые методы по обеспечению информационной безопасности. В складывающихся обстоятельствах, когда со стороны Запада ведется враждебная деятельность, направленная на разрушение всех сфер деятельности нашего государства, существенным и важным представляется определение важнейших направлений по защите национальных интересов России, в том числе и с использованием современных цифровых технологий.

В информационной агрессии против России используются самые разнообразные порталы и сайты, средства массовой информации. На первых стадиях проведения СВО на Украине большая часть аккаунтов в сети Интернет в русском сегменте характеризовалась откровенно антироссийской направленностью.

Проведение такой интенсивной информационной агрессии, позволило Российской Федерации получить незаменимый практический опыт, который важно использовать в целях обеспечения ИБ общества и государства. Такая информационная война целенаправленно контролируется и управляется, масштабно ведется передача искаженной и дезинформирующей информации по каналам глобальных цифровых платформ.

Самым уязвимым направлением сфере ИБ в России можно считать наличие киберпреступлений, слабый уровень профессиональной подготовленности специалистов в этой сфере, отставание отечественных разработок от зарубежных в области информационных и программных технологий.

Такие угрозы представляют серьезную опасность для ИБ, как национальной составляющей национальной безопасности страны.

Таким образом, основные направления по обеспечению информационной безопасности в условиях цифровизации должны быть ориентированы на применение мер, которые обеспечивали бы надежность и устойчивость информационной инфраструктуры. Необходимо на уровне государства и на всех уровнях управления решать вопросы законодательного характера, позволяющие повысить уровень конкурентоспособности и защищенности информационных технологий.

Для нейтрализации угроз в информационной сфере деятельности производственных и коммерческих структур при передаче, хранении, обработке информации необходимо внедрение действенного контроля за осуществлением данных процессов, осуществлять качественную подготовку специалистов в области информационной безопасности.

Перечень используемой литературы и источников:

1. О стратегии национальной безопасности в Российской Федерации [Текст]: Указ Президента Российской Федерации от 02.07.2021 № 400 // Справочно-правовая система «Консультант Плюс».
2. О безопасности [Текст]: федер. закон: [принят 28 декабря 2010 г. № 390-ФЗ (с изменениями от 10 июля 2023 г.)] // НПП «Гарант-Сервис».
3. Об информации, информационных технологиях и защите информации: федер. закон: [принят 8 июня 2006 года. № 149-ФЗ (с изменениями от 31 июля 2023 г.)] // НПП «Гарант-Сервис».
4. Горбенко А.О. Основы информационной безопасности (введение в профессию): учебное пособие для вузов // А.О. Горбенко. – Санкт-Петербург: Интермедио, 2017. – 336 с.
5. Информационные системы и технологии в экономике управления: учеб. для академического бакалавриата // Санкт-Петербургский государственный экономический университет под ред. В.В. Трофимова. – 4-е изд., перераб. и доп. – Москва: Юрайт. – 2017. – 542 с.
6. Минаков А.В. Обеспечение экономической безопасности России в условиях развития цифровой экономики / А.В. Минаков // Экономика и бизнес: теория и практика. – 2019. - № 32 с.19-22.
7. Щеглов А.Ю. Защита информации: основы теории: учебник для бакалавриата и магистратуры / А.Ю. Щеглов, К.А. Щеглов. – Москва: Юрайт. – 2020. – 309 с.

2.8. ПРОБЛЕМЫ ОБЕСПЕЧЕНИЯ ИНФОРМАЦИОННОЙ БЕЗОПАСНОСТИ В РОССИЙСКОЙ ФЕДЕРАЦИИ

Статья посвящается изучению правовых инструментов, используемых для обеспечения национальной безопасности. Проведенный анализ позволяет говорить о наличии угрозы безопасности, связанной с информационным пространством. Стремительное развитие техники в эпоху цифровизации снижает эффективность правового регулирования данной сферы, что подтверждается увеличением числа информационных угроз и нападений. Для разрешения проблемы предлагаются определенные изменения в правовой сфере.
Ключевые слова: безопасность, защита, информационная безопасность (ИБ), информационная угроза, национальная безопасность, нормативно-правовые акты, правовая сфера.

PROBLEMS OF ENSURING INFORMATION SECURITY IN THE RUSSIAN FEDERATION

The article is devoted to the study of legal instruments used to ensure national security. The analysis allows us to talk about the presence of a security threat associated with the information space. The rapid development of technology in the era of digitalization reduces the effectiveness of legal regulation of this area, which is confirmed by an increase in the number of information threats and attacks. Certain changes in the legal sphere are proposed to resolve the problem.
Keywords: security, protection, information security (IS), information threat, national security, regulations, legal sphere.

Безопасность – состояние защищенности наиболее важных общественных и государственных интересов как от угроз внешних, так и от внутренних. С древнейших времен безопасность и общины в целом, и ее членов является приоритетом деятельности государств. Основой построения стратегии дальнейшего развития. По этой причине, деятельность государства по обеспечению национальной безопасности – одна из наиболее важных и сложных, многоаспектных тем для рассмотрения и изучения.

Одно из главных направлений деятельности по обеспечению безопасности связано с изданием и изменением нормативно-правовых актов, призванных регулировать наиболее важные отношения. Эта работа, в свою очередь, происходит только в определенном процессуальном порядке, который может занимать значительный промежуток времени. В то же время, общественные отношения развиваются и изменяются стремительно под воздействием внешних факторов. Данные положения приводят к появлению ситуаций, когда некоторые отношения не урегулированы правом совсем или частично.

На данный момент, существуют следующие нормативные акты, которые являются правовой основой обеспечения национальной безопасности в Российской Федерации:

- Конституция Российской Федерации.
- Общепризнанные принципы и нормы международного права.
- Федеральные конституционные законы Российской Федерации.
- Федеральные законы Российской Федерации.
- Иные нормативно-правовые акты Российской Федерации.
- Законы и иные нормативно-правовые акты субъектов Российской Федерации.
- Нормативно-правовые акты, органов местного самоуправления, принятые в пределах их компетенции в области безопасности.

Если говорить о конкретных нормативно-правовых актах, то это Федеральный закон «О безопасности» от 28.12.2010 № 390-ФЗ; Федеральный закон «О стратегическом планировании в Российской Федерации» от 28.06.2014 № 172-ФЗ; Указ Президента РФ от 02.07.2021 № 400 «О Стратегии национальной безопасности Российской Федерации» («Стратегия»).

«Стратегия» содержит в себе наиболее точный перечень необходимых мероприятий для осуществления задач, способствующих обеспечению безопасности государства во всех сферах. В действующей на данный момент «стратегии», представлены следующие направления обеспечения национальной безопасности:

- Сбережение народа России и развитие человеческого потенциала;
- Оборона страны;
- Государственная и общественная безопасность;
- Информационная безопасность;
- Экономическая безопасность;
- Научно-технологическое развитие;
- Экологическая безопасность и рациональное природопользование;
- Защита традиционных российских духовно-нравственных ценностей, культуры и исторической памяти [2].

Для демонстрации несовершенства существующей правовой системы в области безопасности, обратимся к проблемам в сфере информационной безопасности (ИБ), имеющей большое значение в современную эпоху цифровизации. Общество и государство уже не раз сталкивается с угрозами, связанными с информационным пространством. Один из ярких примеров – киберугрозы. Так, по статистике, только за 1-й квартал 2021 года количество атак увеличилось на 17% по сравнению с 1-м кварталом 2020 года [3]. Также наблюдается тенденция роста количества атак, направленных на различные организации, в том числе и на государственные органы. В ноябре 2021 года Минцифры РФ сообщило об атаке на портал «Госуслуги». Во время проведения атаки пользователи испытывали сложности с вхождением в портал «Госуслуг». Атака была отражена и в настоящее время работоспособность портала полностью восстановлена. А в июле этого же года была подтверждена кибератака на официальный сайт Министерства обороны Российской Федерации. После ее нейтрализации, было установлено, что источник атаки находился за пределами нашей страны. Из вышесказанного можно сделать вывод о возрастающей опасности киберпреступности, поскольку техника становится необходимым условием для полноценного существования общества.

Не меньшую угрозу представляет расширение областей применения криптовалюты. Криптовалюта – электронное платежное средство, не имеющее внешнего материального выражения [4]. Из-за этой особенности у государства имеется довольно ограниченный перечень способов для контроля и управления передвижения криптовалюты. Часто это используется злоумышленниками для совершения незаконных сделок, легализации незаконных доходов, а также финансирования запрещенных организаций. Кроме этого, существование криптовалюты расширяет возможности мошенников в финансовой сфере, что наносит значительный вред государству или создает реальную угроза причинения такого вреда. В современном законодательстве только начала закладываться основа для официального закрепления криптовалюты. Так, в Федеральном законе от 31.07.2020 № 259-ФЗ «О цифровых финансовых активах, цифровой валюте и о внесении изменений в отдельные законодательные акты Российской Федерации» есть легальное определение криптовалюты – цифровая валюта [1]. В этом же акте она признается имуществом. С другой стороны, в законодательстве присутствуют проблемы в отношении правил выпуска и обращения цифровой валюты. Более того, установлен прямой запрет на ее использование в качестве оплаты за товары, услуги и работы. В то же время, совершение гражданско-правовых сделок с использование цифровой валюты разрешено, при условии, что о факте обладания валютой и совершения с ней сделок проинформированы налоговые органы.

Противостояние киберугрозам и обеспечение кибербезопасности являются задачами глобального масштаба, которые остро стоят перед всем мировым

сообществом, а не только перед одним государством. Киберпреступность, изначально применявшаяся только для хищения средств или информации, теперь представляет серьезную угрозу, используемую в политических, корыстных, идеологических и иных целях. Данная ситуация приводит к необходимости активного вмешательства государства. Для обеспечения информационной безопасности требуется увеличение финансирования и расширение инвестирования не только на уровне государства, но и на уровне отдельных организаций и частных лиц, на необходимые мероприятия по защите.

Помимо этого, важно повышение информационной грамотности населения, воспитание и становление информационной культуры. Только имея представление о том, чем являются киберугрозы, какой вред они могут принести и от кого они исходят, возможно будет выработать эффективную систему поведения. Также в данном вопросе важно проведение политики по популяризации технологий и создание условий для благоприятной технологической среды на всей территории Российской Федерации. С вышеназванными мероприятиями тесно связана необходимость обеспечения определенных правовых гарантий лиц в информационном пространстве. Например, право на возмещения вреда от причиненного вреда, право на обращение в органы государственной власти за защитой, право на защиту своих персональных данных и т.д. Большое значение имеет создание специализированных организаций по борьбе с киберугрозами, наращивание кадрового потенциала и повышение конкурентоспособности Российской Федерации в информационной сфере.

Пока в государстве не выстроена четкая информационная политика, пока правовые акты в данной сфере не соответствуют техническим существующим возможностям, и пока информационная грамотность населения не достигнет допустимого предела и не будет создано четкого механизма возмещения вреда, причиненного гражданину, у нас нет возможности говорить о полном и эффективном обеспечении безопасности в информационном пространстве.

Перечень использованной литературы и источников:

1. Российская Федерация. Законы. О цифровых финансовых активах, цифровой валюте и о внесении изменений в отдельные законодательные акты Российской Федерации: федер. закон от 31.07.2020 № 259-ФЗ // Собрание законодательства Российской Федерации. – 2020. - Выпуск № 31. – Ст. 5018.

2. Российская Федерация. Президент. О Стратегии национальной безопасности Российской Федерации: Указ Президента РФ от 2 июля 2021 г. № 400 // Собрание законодательства Российской Федерации. – 2021. - Выпуск № 27. – Ст. 535177.

3. Актуальные киберугрозы: I квартал 2021 года // ПАО «Группа Позитив»: сайт. – Москва, 2022. – URL: https://www.ptsecurity.com/ru-ru/research/analytics/cybersecuritythreatscape-2021-q1/ (дата обращения 15.02.2023).

4. Криптовалюта (крипта): что это такое и как на ней заработать // Финам. – URL: https://www.finam.ru/ (дата обращения 17.02.2023).

2.9. ПРОТИВОДЕЙСТВИЕ ЯПОНИИ В ИНФОРМАЦИОННО-ПСИХОЛОГИЧЕСКОЙ ВОЙНЕ КАК СОСТАВНОЙ ЧАСТИ ИНФОРМАЦИОННОЙ БЕЗОПАСНОСТИ РОССИ (на примере Сахалинской области)

Статья посвящена противодействию японской информационно-психологической войне против России как составной части информационной безопасности страны. Авторы на основании документов приходят к выводу, что задачу сохранения территориальной целостности государства, обычно решаемую центральными властями, в современных условиях общественности и властям Сахалинской области пришлось (прежде всего, по отношению к своей территории) ставить не только перед собой, но и перед федеральными властями. Причинами этого стали непоследовательность политики центральных властей в отношении судьбы Курильских островов, приграничное положение региона, наличие территориальных претензий Японии, географическая труднодоступность Курил.

Ключевые слова: информационная безопасность, информационно-психологическая война, Курильские острова, Россия, Сахалинская область, территориальные притязания Японии, Япония.

COUNTERING JAPAN IN INFORMATION-PSYCHOLOGICAL WARFARE AS A COMPONENT OF RUSSIA'S INFORMATION SECURITY (using the example of the Sakhalin region)

The article is devoted to countering the Japanese information-psychological war against Russia as an integral part of the country's information security. The authors, based on the documents, come to the conclusion that the task of preserving the territorial integrity of the state, usually solved by the central authorities, in modern conditions, the public and the authorities of the Sakhalin region had to set (primarily in relation to their territory) not only to themselves, but also to the federal authorities. The reasons for this were the inconsistency of the policy of the central authorities regarding the fate of the Kuril Islands, the border position of the region, the presence of territorial claims of Japan, and the geographical inaccessibility of the Kuril Islands.
Key words: information security, information-psychological warfare, Kuril Islands, Russia, Sakhalin region, territorial claims of Japan, Japan.

Информационная война Японии против России имеет давнюю историю, носит плановый и системный характер, всячески поддерживается, финансируется и ведется в основном государством. Информационная война может быть определена как использование и управление информацией с целью получения конкурентоспособного превосходства над противником в различных сферах, а противодействие в этой войне – как часть информационной безопасности России. Без единого выстрела, можно добиться значительного превосходства над противником, сбросив в средства массовой информации и интернет заведомо неправильную информацию, что, например, происходит и с использованием термина «северные территории» японской пропагандой.

Применение термина «северные территории», именование части Малой Курильской гряды прежним японским названием «Хабомаи», использование безвизовых обменов как средства «мягкой силы», законодательное объявление южных Курил территорией Японии, картографическая агрессия – все это требует, но не всегда находит реакции со стороны Российской Федерации. В нашей стране пока не существует специализированного органа по сохранению территориальной целостности и противодействию информационно-психологической войне в этой сфере, хотя нужда в этом органе имеется.

Сахалинская область является главным форпостом противодействия Японии в ее информационной войне по территориальному вопросу. Органы власти и управления области на протяжении 1990-х – 2000-х годов всегда принимали в этом активное участие.

Тема японских притязаний и противодействия им достаточно специфична и требует как специальной подготовки, так и издания соответствующей литературы. С пониманием этого еще в 1992 году с помощью администрации Сахалинской области была издана книга известного специалиста-японоведа Игоря Латышева «Покушение на Курилы». Сахалинский областной Совет народных депутатов приобрел для депутатов часть тиража, вооружив их знанием предмета [2].

Одним из средств противодействия в информационной войне стало установление памятных знаков, как это было сделано на острове Танфильева Малой Курильской гряды в ноябре 1997 года, в честь 300-летия открытия Курильских островов русскими людьми. Доставку памятника к месту установки взяли на себя военные летчики: до Кунашира монумент долетел на самолете, а дальше, до острова Танфильева – на вертолете. Винтокрылой машине пришлось совершить четыре рейса, чтобы доставить на островок цемент, арматуру, необходимые для работы инструменты.

Японская сторона активно использует в пропагандистских целях безвизовый обмен между жителями Курильских островов и Японией. В обращении Сахалинской

областной Думы к тогдашнему министру иностранных дел России Е.М. Примакову от 2 декабря 1997 года указывалось: «становится очевидным, что японская сторона постепенно отходит от заявленных принципов безвизового обмена и создает выгодные для себя условия для оказания пропагандистского воздействия на жителей островов. При формировании делегаций японские организаторы активно включают в их состав представителей государственных органов – МИДа Японии, депутатов парламента, депутатов префектуральной Ассамблеи, руководства губернаторства Хоккайдо, служащих муниципалитета округа Нэмуро, наиболее близко расположенного к Курильским островам – в ущерб рядовым гражданам, желающим посетить острова».

При этом предлагался комплекс мер противодействия, который с помощью МИД РФ был впоследствии реализован. Он включал в себя предложение об обязательном согласовании через МИД России состава японских делегаций; при организации безвизовых поездок нужно было предоставлять органам государственной власти Сахалинской области полномочия согласовывать сроки, места посещения и списки участников. Также предлагалось: направлять представителей органов государственной власти области для участия в переговорах по подведению итогов и согласованию планов развития безвизовых обменов, которые проводятся ежегодно в январе; делегировать представителям органов государственной власти Сахалинской области, направляемым на подведение итогов безвизовых обменов, право представления Курильского и Южно-Курильского районов (по согласованию); согласовывать позицию российской стороны по направлениям развития безвизовых обменов путем проведения консультаций [1; 3; 4].

11 июля 2003 года Сахалинская областная Дума приняла обращение к Президенту России «Об использовании японской стороной безвизовых обменов для проведения идеологических акций в отношении жителей южных Курил».

В обращении отмечалось, что японская сторона активно использует безвизовые обмены для идеологического воздействия на жителей Курильских островов с целью формирования предпосылок для передачи островов Японии.

С японской стороны основными организаторами направления и приема безвизовых делегаций являются МИД Японии, «Всеяпонский Совет по развитию связей с четырьмя северными территориями» (ВЯС–ЧСО), «Хоккайдский Совет по развитию связей с четырьмя северными территориями» (Хок–ЧСО), Управление по вопросам «северных территорий» губернаторства Хоккайдо.

Указанными организациями под руководством МИДа Японии разрабатываются программы пребывания российских граждан, обязательным элементом которых являются дискуссии и лекции по территориальному размежеванию России и Японии. В ходе таких мероприятий японские специалисты в выгодном для Японии свете акцентируют внимание российских участников обменов на том, что СССР, а ныне Россия «незаконно оккупировала и владеет Курильскими островами». Психологическое воздействие закрепляется вручением россиянам сувениров и печатной продукции на русском и японском языках с надписями реваншистского содержания, искаженным изображением Государственной границы РФ, призывами вернуть Японии Курильские острова. С российской стороны вся нагрузка по безвизовым отношениям лежит на администрации Южно-Курильского района, которая при всем желании не имеет возможности адекватно противостоять японской «государственной машине».

С японской стороны в состав делегаций включаются, прежде всего, активисты движений «за возвращение четырех островов», действующих в каждой префектуре Японии. Важным критерием включения кандидата в безвизовую поездку является участие в мероприятиях идеологического воздействия на курильчан, распространение соответствующих печатных изданий и символики.

В частности, в безвизовой делегации, побывавшей на Курилах в июне 2003 года и насчитывавшей 65 человек, только трое участников являлись родственниками

японцев – бывших жителей Курильских островов, остальные – активисты реваншистских движений, депутаты Парламента Японии, сотрудники МИДа, функционеры ВЯС–ЧСО, Хок–ЧСО, а также журналисты.

Учитывая изложенное, Сахалинская областная Дума в целях защиты жителей Южно-Курильского района Сахалинской области от идеологической и картографической экспансии предложила:

1. Пересмотреть сформировавшийся в советском и российском руководстве в 1990-е годы подход к вопросу о принадлежности южных Курил, который признает наличие территориальной проблемы в отношениях с Японией.

2. Поручить МИД РФ, ФПС, ФСБ обеспечить должный контроль за въездом и выездом безвизовых делегаций и воспрепятствовать ввозу в Российскую Федерацию картографической продукции с искаженным изображением государственной границы Российской Федерации, а также материалов, содержащих призывы к передаче Японии южных Курильских островов [6]. Правда, в тот раз никаких конкретных действий со стороны Правительства РФ не последовало. Ознакомившись с текстом Московской декларации от 13 ноября 1998 года (Ельцин – Обути), депутаты Сахалинской областной Думы были удивлены тем, что часть Малой Курильской гряды, расположенной юго-западнее острова Шикотан, упоминается в декларации под японским названием «Хабомаи». Сахалинская областная Дума в заявлении от 3 декабря 1998 года сочла, что применение только японских географических названий в межправительственных документах некорректно, и заявила, что настаивает на использовании в официальных документах российских географических названий [20, 156-157]. Как результат из российских официальных документов название «Хабомаи» исчезло.

В Рекомендациях парламентских слушаний, проведенных в Южно-Сахалинске в сентябре 2001 года, Государственной Думе ФС РФ предлагалось принять поправки в законы Российской Федерации о средствах массовой информации и рекламе, регулирующие порядок использования географического изображения территории Российской Федерации и ее частей. Одновременно Правительству России предлагалось ограничить пропагандистскую деятельность Посольства Японии в России и подчиненных ему фондов через установление запретов, аналогичных запретам, установленным в Японии для деятельности наших дипломатов и средств массовой информации [20, 17-20]. Эти рекомендации были приняты Государственной Думой 18 марта 2002 года [22, 70-78].

В 2001 году в Сахалинской области было зафиксировано несколько случаев распространения материалов с искаженными изображениями этого региона (корейская фирма «Янджи Сангса», японская фирма «Mitsui&Co, LTD» («Мицуи Буссан»), компания «Сахалин Энерджи Инвест Компани ЛТД» – ежедневники; Генеральное консульство Японии – журнал «Ниппония» № 17 за 2001 год).

В этой связи Сахалинская областная Дума в ноябре 2001 года обратилась к послу Республики Корея, Генеральному консулу Японии в Южно- Сахалинске и Президенту России. В обращении к Президенту РФ указывалось, что распространение этого журнала Генеральным консульством Японии на территории России – это недружественный шаг, оскорбляющий национальные чувства россиян, посягающий на территориальную целостность страны, закрепленную статьей 4 Конституции Российской Федерации, поэтому областная Дума отказалась принять этот журнал и 9 ноября 2001 года вернула его в Генеральное консульство Японии в г. Южно-Сахалинске [20, с. 173-177]. В обращении отмечалось, что такого рода картографическая экспансия не безобидна.

Во-первых, применительно к Японии, следует, видимо, констатировать нарушение пункта 3 Совместной Декларации СССР и Японии от 19 октября 1956 года. Согласно последней части этого пункта, СССР и Япония взаимно обязуются не

вмешиваться прямо или косвенно во внутренние дела друг друга по любым мотивам экономического, политического или идеологического характера.

Во-вторых, у населения страны этот факт вызывает ощущение бездеятельности государства в отношении действий, в откровенной (наглядной) форме демонстрирующих посягательство на суверенитет России, целостность и неприкосновенность ее территории (Ст. 4 Конституции РФ). Это снижает «порог чувствительности», способствует привыканию к экспансионизму соседнего государства.

Аналогичное письмо было направлено Министру иностранных дел Российской Федерации И.С. Иванову 19 ноября 2001 года.

Ответ на оба письма был получен от заместителя министра иностранных дел Российской Федерации А. Лосюкова [20, с. 179-180]. МИД России сообщил, отвечая на Обращение Думы, что в этой связи привлек внимание посольств Республики Корея и Японии к недопустимости повторения подобных действий учреждениями или гражданами этих стран. 20 ноября 2001 года было также сделано заявление для печати, в котором распространение в России представителями РК и Японии карт с искаженным изображением территориальной принадлежности южных Курильских островов было расценено как действие, не способствующее укреплению добрососедства, дружбы и доверия между Россией и Японией, наносящее ущерб межгосударственным отношениям [20, с. 175-176].

Учрежденная Правительством Российской Федерации «Российская газета» в номере 91 (2959) от 24 мая 2002 года в статье под заголовком «Известно – когда, неизвестно – кто» на 28 странице под видом карты-схемы городов, в которых будет проходить чемпионат мира по футболу 2002 года, поместила карту «японских притязаний на сопредельные территории», в которую включены территории двух муниципальных образований Сахалинской области Российской Федерации – Курильского и Южно-Курильского районов (острова: Итуруп, Кунашир, Малая Курильская гряда). В этой связи Сахалинская областная Дума 6 июня 2002 года обратилась к министру по делам печати, телерадиовещания и средств массовых коммуникаций Российской Федерации М.Ю. Лесину с предложением о проведении служебного расследования и к редакции «Российской газеты» с требованием о принесении официальных извинений жителям Российской Федерации и Сахалинской области [5, 11].

Этот вопрос был рассмотрен Сахалинской областной Думой в порядке контроля 18 июля 2002 года [5; 11].

В связи с неоднократностью таких случаев 21 декабря 2006 года областная Дума поставила перед Роскартографией и Генеральной прокуратурой РФ вопрос об административной ответственности руководства «Российской газеты» [16, с. 432-434].

«Российская газета» 18 января 2007 года после статьи «Карта – точное название» под рубрикой «От редакции» официально принесла извинения депутатам Сахалинской областной Думы. В связи с этим Роскартография как лицензирующий орган в области геодезии и картографии отложила возбуждение дела о приостановлении действия лицензии на картографическую деятельность, выданной «Российской газете», а также о привлечении должностных лиц газеты к административной ответственности.

В день принесения извинений – 18 января 2007 года – дальневосточное представительство ФГУ «Редакция «Российской газеты» выпустило специальное иллюстрированное издание «Дальний Восток в лицах» и поместило в нем карту Дальневосточного федерального округа без изображения Малой Курильской гряды. Публикация не являлась частной ошибкой регионального представительства, так как в выходных данных специально оговорено, что цветные тематические страницы, включая и данную страницу, являются составной частью «Российской газеты» и распространяются только в составе газеты.

В этой связи Сахалинская областная Дума 15 марта 2007 года обратилась в Правительство РФ с предложением за систематическую антироссийскую и антиконституционную пропаганду освободить главного редактора «Российской газеты» В.А. Фронина от должности [16, с. 442-447].

Сахалинской областной Думой 24 сентября 2002 года было обсуждено название такого подразделения Римско-католической церкви как «Апостольская администратура Восточной Сибири и Префектуры Карафуто». Было констатировано, что действиями представителей Римско-католической церкви на территории Сахалинской области продолжают нарушаться конституционные права свободы совести и вероисповедания граждан России.

Так, органами юстиции было установлено, что священником Римско-католической церкви Ярославом Вишневским в средства массовой информации Сахалинской области в конце 2001 года направлена заметка по поводу рождественских мероприятий за подписью Епископа Ежи Мазура Апостольской администратуры Восточной Сибири и Префектуры Карафуто. В связи с указанной публикацией в Управление Министерства юстиции Российской Федерации по Сахалинской области и прокуратуру Сахалинской области поступали многочисленные жалобы от населения области, органов власти. Наименование «Префектура Карафуто» употреблялось Японией в период оккупации южного Сахалина. Такое вольное переименование Сахалинской области оскорбляло национальные чувства россиян, в частности населения этого региона, и могло толковаться как недружественный шаг, расценивающийся как посягательство на территориальную целостность страны.

Папа Римский после ноты МИД РФ, инициированной сахалинцами, был вынужден исключить из названия администратуры упоминание префектуры Карафуто [10].

Еще одним из способов противодействия информационной войне является присвоение безымянной бухте на острове Танфильева Малой Курильской гряды наименования «бухта Чичерина», принятого Сахалинской областной Думой 25 марта 2004 года. Это наименование было присвоено бухте в честь морского офицера Павла Андреевича Чичерина, командовавшего высадкой десанта на ряд островов Малой Курильской гряды в 1945 году [12].

В 2004 году администрация Сахалинской области обнаружила, что на карте России, размещенной на сайте Президента Российской Федерации, не изображены Курильские острова. После обращения депутата Сахалинской областной Думы на имя Президента РФ ошибка была в июле 2004 года исправлена [16, с. 338].

С 2005 года депутаты Сахалинской областной Думы начали координировать свою деятельность по противодействию японским притязаниям с правительственными органами Республики Корея, которые тоже имеют территориальные проблемы с Японией по поводу острова Токдо [16, с. 377].

В рамках подготовки к празднованию 60-й годовщины освобождения южного Сахалина и Курильских островов от японских милитаристов и окончания Второй Мировой войны 30 июня 2005 года областной оргкомитет «Победа» принял предложение по репринтному выпуску газеты «Правда» от 2 сентября 1945 года с текстом Указа Президиума Верховного Совета СССР о Дне Победы над Японией и материалами о капитуляции Японии [16, с. 392].

В 2005 году Сахалинская областная Дума обратила внимание на искажение первым каналом Центрального телевидения границ России и распространение одобренного Министерством образования РФ учебного пособия с картой России, на которой отсутствовали Калининградская область и Курильские острова. Как сообщила Дирекция информационных программ «Первого канала», корреспонденту, который ввел в заблуждение всю страну относительно ее границ, объявили выговор, указали на

необходимость использования в своих материалах более точных формулировок и лишили премии за месяц [15].

Известным российским скульптором Зурабом Церетели к 2006 году был изготовлен для установки в Ялте памятник «ялтинской тройке» (Сталин, Черчилль, Рузвельт). В числе принятых «тройкой» в 1945 году решений предусматривалось вступление СССР в войну с Японией, возвращение Советскому Союзу южного Сахалина и передача Курильских островов. После отказа украинских властей, которым тогда принадлежал Крым, принять памятник, возник вопрос о месте его установки. Было предложено установить в Южно-Сахалинске этот памятник персонализированному согласию союзников – в знак уважения к принятому решению и как фактор обеспечения территориальной целостности этих российских земель в будущем (превращение «ялтинской тройки» в «тройку пограничников» имело бы несомненное информационно-наступательное значение). От автора памятника было получено согласие на его установку в Южно-Сахалинске. Это предложение было широко поддержано общественностью [16, с. 413-414]. Хотя эта идея и не была реализована, она не утратила своего значения и может быть использована в рамках информационного противодействия Японской экспансии.

На основании большого фактического материала, с учетом опыта безвизовых обменов, целенаправленных действий японской стороны, ряда примеров некритического использования российской прессой иностранных карт, Сахалинская областная Дума 9 ноября 2006 года приняла постановление с предложением Правительству Российской Федерации выработать систему мер противодействия картографической агрессии и иным видам информационной агрессии со стороны Японии, включающую:

1) выполнение пунктов 11-19 Рекомендаций Правительству Российской Федерации, принятых на парламентских слушаниях, на тему: «Южные Курилы: проблемы экономики, политики и безопасности», прошедших 18 марта 2002 года в Государственной Думе Федерального Собрания Российской Федерации;

2) обеспечение защиты от специальной психологической обработки российских граждан в рамках безвизовых обменов, определенных обменными письмами Министров иностранных дел СССР и Японии от 14 октября 1991 года;

3) пересмотр порядка и условий безвизовых обменов (по сути, неравноправных), в ходе которых жители только двух из трех муниципальных образований, расположенных на Курильских островах, имеют право на групповое безвизовое посещение Японии, а жители Сахалина и северных Курил не имеют аналогичной возможности;

4) денонсацию части 2 статьи 9 Советско-японской Декларации 1956 года – в связи с систематическими и грубыми нарушениями японской стороной статей 3 и 6 названной Декларации [17]. Хотя эти предложения и не были реализованы, ни одна из этих рекомендаций не потеряла актуальности и сегодня.

Внефракционное депутатское объединение «За Российские Курилы!» при планировании своей деятельности на 2007 год основным направлением работы считало информационно-пропагандистское, что видно из его решения от 17 января 2007 года [16, с. 435-436]. Уже 21 января 2007 года 11 депутатов Сахалинской областной Думы обратились с Открытым письмом в отношении антироссийской пропаганды в российских средствах массовой информации к Президенту РФ как к Председателю оргкомитета «Победа» [16, с. 436-440].

Направляя руководству страны резолюцию митинга, прошедшего в Южно-Сахалинске 7 февраля 2007 года, организаторы указали на наибольшую опасность информационно-психологической войны, ведущейся против России. Элементами этой войны названы картографическая агрессия, преуменьшение объема японских

притязаний («4 острова», хотя их около 20), непризнание итогов Второй мировой войны и т.п. [16, с. 440-442].

15 марта 2007 года Сахалинская областная Дума провела анализ исполнения постановлений, касающихся картографической агрессии. В числе важных результатов было отмечено, что ее руководитель обратился ко всем субъектам геодезической и картографической деятельности и пользователям официального сайта Роскартографии с Открытым письмом, предлагая не допускать использования в своей деятельности картографических материалов с искажениями в показе территории Российской Федерации и (или) в написании наименований российских географических объектов [13]. Эти решения Сахалинской областной Думы контролировались и в дальнейшем [16, с. 452-455].

В газете «Экономика» 12 декабря 2007 года на схеме территории части Дальневосточного федерального округа, приложенной к статье обозревателя «Российской газеты» Т. Зыковой «На востоке страны появилась мощная газовая империя», южные и средние Курилы были обозначены как территория Японии, остальные острова Курильской гряды – не изображены. Похожую публикацию допустила газета «Коммерсант». Это обусловило резкую публичную реакцию Сахалинской областной Думы в постановлении от 7 февраля 2008 года [7].

Губернатором и Правительством Сахалинской области в 2009 году была запланирована, а в 2010 году проведена международная конференция, посвященная 65-летию окончания Второй мировой войны. В 2015 году проведена вторая конференция, посвященная уже 70-летию окончания Второй мировой войны. На этой конференции прозвучало предложение переименовать Сахалинскую область в Сахалино-Курильский край. Термин «край» утвердился в нашей стране исторически для больших по площади пограничных регионов с наличием национальных автономий или значительных внутренних природно-географических различий. В случае с предлагаемым Сахалино-Курильским краем все указанные признаки (кроме автономий) присутствуют. Остров Сахалин и Курильская гряда – это большие, различные по своей геоморфологии структуры, разнесенные друг от друга на весьма значительные расстояния. Здесь главным доводом является внятная топонимическая привязка Курильских островов к уже достаточно широко известному названию пограничного региона России, образованного по итогам Второй мировой войны [21, с. 121]. В дальнейшем эта идея получила развитие.

Как отмечалось, основная идея переименования области состоит в демонстрации возросшей роли Курильских островов для нашего региона и Российской Федерации. Для этого предлагалось ввести законодательными актами (Конституция РФ, Указ Президента РФ, законодательство области) и картографическими средствами в общественное сознание, в том числе и зарубежное, образы принадлежности Курил нашему субъекту Российской Федерации и их неразрывного единства; продвижение обновленного образа области (края).

В качестве следствий переименования можно было бы с уверенностью прогнозировать:

– укрепление территориальной целостности Российской Федерации;

– демонстрацию неизменности итогов Второй мировой войны в северо-восточной Азии;

– повышение самооценки жителей Курильских островов;

– сокращение числа случаев, когда в средствах массовой информации будет искажаться принадлежность Курильских островов;

– значительно более адекватное восприятие федеральными структурами и населением страны специфического (не просто островного, а многоостровного) характера Сахалинской области, требующего соответствующего отношения, подхода и

финансирования; продолжение действующей ФЦП «Социально-экономическое развитие Курильских островов» и продление ее на последующие периоды;

– реализацию идеи создания на Курилах особой экономической (таможенной, порто-франко и т.п.) зоны, дающей дополнительный импульс к их самобытному развитию;

– увеличение интереса к Сахалинской области (Сахалино-Курильской области или краю), укрепление и продвижение ее имиджа [19].

Принципиально важными явились изменения в Уставе Сахалинской области, имеющем значение конституции субъекта Российской Федерации, внесенные 24 декабря 2010 года. В структуру Устава по инициативе Сахалинского областного отделения Русского географического общества введено Приложение, содержащее «Описание состава Сахалинской области». В этом Описании впервые дан перечень островов Сахалинской области, в том числе раздельно по Большой и Малой Курильской грядам. Нормативно-значимое перечисление Курильских островов от полуострова Камчатка до японского острова Хоккайдо не оставляет места для пропагандистского ложно-географического образования «северные территории».

Кроме того, стало понятно, что Малая Курильская гряда – это не два острова, называемые претендующей стороной и ее сторонниками «Шикотан и Хабомаи», а два десятка островов и островных групп, имеющих российские названия [8].

С 2012 года Сахалинским областным отделением Русского географического общества при поддержке Правительства области и Сахалинской областной Думы ведется регулярная целенаправленная работа по имянаречению безымянных географических объектов на Курильских островах, способствующая русификации карты области, увековечению героев войны с Японией, видных государственных деятелей (острова Деревянко, Громыко, Гнечко, Щетининой, мысы Маршала Крылова, Адмирала Юмашева, Пуркаева, Радужанова, Воронова, Гурьева и др.) [14; 9; 18]. Все это имеет и информационно-просветительский аспект.

Важнейшим элементом противодействия информационной войне Японии против России является контроль сахалинскими властями информационного пространства. Администрация области, обнаружив, что крупная компания «LG Elektronics» – Россия в буклете «Бытовые кондиционеры LG 2010» разместила карту-схему территории Российской Федерации без показа Курильских островов, направила компании письмо, в котором указала, что печатные издания, в которых содержатся искаженные картографические изображения и пометки, создают угрозу информационной безопасности Российской Федерации. 16 мая 2012 года компания сообщила, что «в ближайшее время ООО «ЛГ Электроникс РУС» предпримет все возможные меры по изъятию некорректной карты из каталогов нашей продукции и по скорейшему урегулированию сложившейся ситуации со всем уважением к государственному устройству Российской Федерации» [16, с. 495-496].

Чрезвычайно важным для данной тематики можно считать митинг сахалинцев и курильчан в защиту территориальной целостности России, прошедший 22 декабря 2018 года. В пункте 4 Резолюции участники митинга потребовали от Правительства РФ принятия Правил публичного изображения территории Российской Федерации в целях противодействия картографической агрессии Японии, поддерживаемой отдельными российскими средствами массовой информации, а от Федерального Собрания Российской Федерации – введения административной ответственности за публичное (в СМИ или иным способом) искаженное изображение территории Российской Федерации, в частности, без территорий, на которые официально претендуют другие государства [16, с. 533-539].

Таким образом, задачу сохранения целостности государства, обычно решаемую именно центральными властями, общественности и властям Сахалинской области Российской Федерации пришлось (прежде всего, по отношению к своей территории)

ставить перед собой и федеральными властями. Стимулирующими факторами для этого стали колебания центральных властей в отношении судьбы островов, приграничное положение региона, наличие территориальных претензий Японии как сопредельного государства, географическая труднодоступность Курильских островов, временами доходившая до их изолированности. В ряду государственно-правовых субъектов (партий, территорий и т.д.) Сахалинская область была и остается объективно самым заинтересованным и мотивированным субъектом. Поэтому именно она и взяла с 1990 года на себя роль центра силы, давления и концентрации усилий по самосохранению, а через это – к сохранению территориальной целостности России, ее информационной безопасности.

Перечень использованной литературы и источников:

1. Ведомости Сахалинской областной Думы. – 1997. – № 6.
2. ГИАСО. Ф. 1183. Оп. 1.Ед. хр. 166. Л. 68, 70, 151.
3. Губернские ведомости – 1997. – 6 декабря. – № 98-99.
4. Губернские ведомости – 1997. – 7 ноября. – № 87.
5. Губернские ведомости – 2002. – 16 августа. – № 155 (1556).
6. Губернские ведомости – 2003. – 5 августа. – № 157.
7. Губернские ведомости – 2008. – 15 февраля. – № 327 (2994).
8. Губернские ведомости – 2010. – 29 декабря. – № 238 (3685).
9. Губернские ведомости – 2016. – 15 апреля. – № 65 (4953).
10. Губернские ведомости – 2002. – 11 октября. – № 195 (1596).
11. Губернские ведомости – 2002. – 3 июля. – № 122 (1523).
12. Губернские ведомости – 2004. – 25 мая. – № 113.
13. Губернские ведомости – 2007. – 23 марта. – № 51.
14. Губернские ведомости – 2015. – 20 июня. – № 105 (4753).
15. Для сахалинцев и курильчан. – 2005. – 26 октября. – № 42 (163).
16. Курильский аспект. Деятельность органов власти и общественности Сахалинской области по сохранению территориальной целостности России. 1947–2019 годы: сборник документов и материалов / Автор-составитель С.А. Пономарев. – Южно-Сахалинск: КорКи'С, 2019. – 597 с.
17. Правда. – 2006, от 17–20 ноября – № 127 (29035).
18. Российская газета. – 2017, от 17 февраля (Столичный выпуск. – № 7202 (36)).
19. Советский Сахалин. – 2011, от 28 июня. – № 83.
20. Советско-японская Декларация 1956 года и проблемы национальной безопасности Российской Федерации. – Южно-Сахалинск, 2002. – 332 с.
21. Уроки Второй мировой войны и современность: Материалы международной научно-практической конференции, посвященной 65-летию окончания Второй мировой войны. 2-3 сентября 2010 года. – Москва, 2011. – 404 с.
22. Южные Курилы: проблемы экономики, политики и безопасности. Материалы парламентских слушаний. 18 марта 2002 года. – Москва: Издание Государственной Думы, 2003. – 80 с.

2.10. ВОПРОСЫ ПОВЫШЕНИЯ БЕЗОПАСНОСТИ РАБОТЫ СОТРУДНИКОВ ПОЖАРНОЙ ОХРАНЫ

Сотрудники структурных подразделений, которые непосредственно учувствуют в ликвидации как ЧС, так и ее последствий в процессе выполнения своей профессиональной деятельности подвергаются различным вредным и опасным факторам. Повышение безопасности работы сотрудников пожарной охраны достигается комплексом методов управления и принятия необходимых эффективных решений в области охраны труда.

Ключевые слова: анализ производственного травматизма, мероприятия направленные на повышение безопасности работы пожарных, сотрудники пожарной охраны.

ISSUES OF IMPROVING THE SAFETY OF THE WORK OF FIRE PROTECTION OFFICERS

Employees of structural divisions who directly participate in the elimination of both emergencies and its consequences in the course of their professional activities are exposed to various harmful and dangerous factors. Improving the safety of fire protection personnel is achieved by a set of

management methods and making the necessary effective decisions in the field of occupational safety.
Keywords: fire protection officers, analysis of occupational injuries, measures aimed at improving the safety of firefighters.

В пожарной охране для повышения безопасности сотрудников должен систематически применяться весь предусмотренный нормативной базой комплекс методов управления: идеологических, организационно-распорядительных, социально-экономических и социально-психологических, с их программно-материальным обеспечением для быстрого анализа, поступающей внешней и внутренней информации и принятия необходимых эффективных решений в области охраны труда.

Для оценки эффективности работы по охране труда в Главном управлении (ГУ) МЧС России по любой области и пожарных частях, как его структурных подразделений изучают статистику несчастных случаев, произошедших с личным составом при исполнении служебных обязанностей за последние 3 года, так как основным показателем состояния охраны труда является количество несчастных случаев, произошедших с личным составом при исполнении служебных обязанностей. На рис. 1 показано количество несчастных случаев с личным составом Федеральной противопожарной службы (ФПС) ГУ МЧС России по Тамбовской области в период с 2020 до 2022 годы.

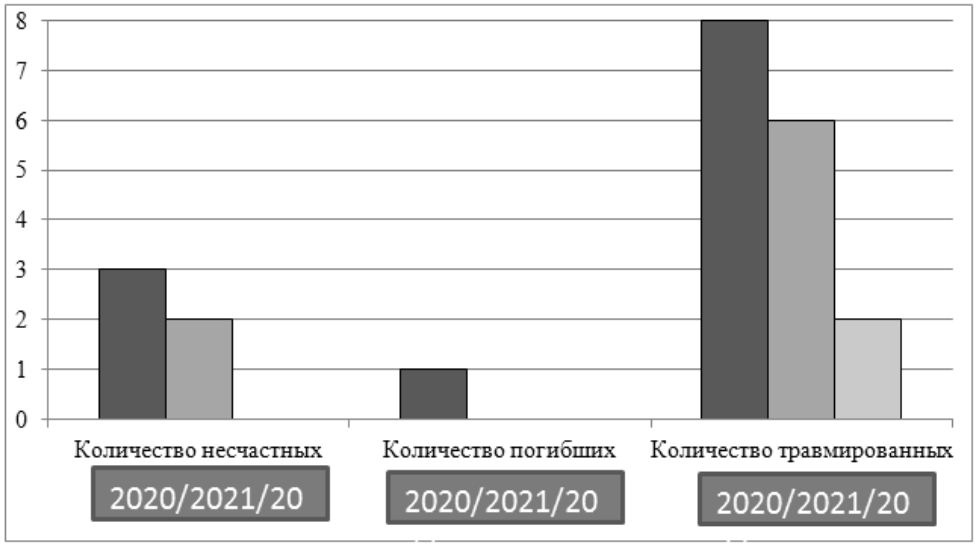


Рисунок 1 – Количество несчастных случаев с личным составом ФПС ГУ МЧС России по Тамбовской области в период с 2020 до 2022 годы

Так же проводят анализ нормативной базы, принятой ГУ в области охраны труда. В ходе изучения приказов Главного управления установлено, что нормативно-правовая база в области охраны труда соответствует требованиям законодательства.

Проведя изучения статистики несчастных случаев с личным составом ФПС ГУ МЧС России по Тамбовской области в период с 2020 до 2022 годы, и проведя анализ принятой нормативно-правовой базы по охране труда, дополнительных мероприятий, можно сделать вывод, что работа Главного управления является достаточной и эффективной.

В соответствии с приказами Главного управления на постоянной основе выполняются следующие мероприятия:

1. В Главном управлении служба управления охраной труда трехуровневая. Управление охраной труда на первом уровне осуществляет должностное лицо, назначенное начальником структурного подразделения (начальник пожарно-спасательной части). Контроль на первом уровне проводится ежедневно. Управление охраной труда на втором уровне в соответствии с имеющимися полномочиями

осуществляет начальник структурного подразделения (начальник Управления пожаротушения и проведения аварийно-спасательных работ). Контроль осуществляется ежеквартально. Управление охраной труда на третьем уровне осуществляет начальник Главного управления. Контроль проводится не реже одного раза в год;

2. Начальник пожарно-спасательной части (ПСЧ) назначается ответственным за охрану труда и организацию работы по охране труда;

3. Заместитель начальника ПСЧ назначается ответственным за проведение первичного, повторного, целевого инструктажей по охране труда, программы инструктажей разработаны и утверждены, инструкции по охране труда разработаны и утверждены, записи о проведенных инструктажах проставляются в журнале инструктажей по охране труда. Периодичность проведения инструктажей определена Постановлением Правительства РФ от 24 декабря 2021 г. № 2464 «О порядке обучения по охране труда и проверки знания требований охраны труда»;

4. В ПСЧ разработаны и введены в действие программы инструктажей по охране труда: первичного (повторного) инструктажа на рабочем месте, разработаны инструкции по охране труда по видам работ и по профессиям);

5. Заместитель начальника ПСЧ назначается ответственным за электрохозяйство;

6. Начальник ПСЧ, его заместитель, начальники караулов и командиры отделений (лица, выступающие в роли руководителей тушения пожара) проходят проверку знаний требований охраны труда по программу «Охрана труда для руководителей и специалистов», в объеме 40 часов;

7. Ежеквартально в ПСЧ проводится «День охраны труда», в ходе данного мероприятия у личного состава принимаются зачеты по знаниям правил охраны труда, производится комиссионное обследование здания, территории пожарного депо, пожарной техники и пожарно-технического вооружения, по итогам проведения «Дня охраны труда» составляется акт, указываются мероприятия направленные на устранение выявленных недостатков, данный акт рассматривается на общем собрании личного состава ПСЧ;

8. В соответствии с требованиями Федерального закона от 28.12.2013 № 426-ФЗ «О специальной оценке условий труда», на основании приказа ГУ МЧС России по Тамбовской области от 10.06.2022 № 555 «О проведении специальной оценки условий труда в ГУ МЧС России по Тамбовской области» проводится специальная оценка условий труда. По результатам, которой работникам ПСЧ, непосредственно принимающим участие в тушении пожаров и проведении аварийно-спасательных работ присваивается соответствующий класс условий труда (например, вредные условия труда класса 3.3), устанавливается повышенный размер оплаты труда, ежегодный дополнительный оплачиваемый отпуск (7 дней), сокращена продолжительность рабочего времени, кроме того утверждается дополнительный рекомендуемый перечень мероприятий по улучшению условий труда;

9. Ежегодно сотрудники ПСЧ принимают участие в проведении смотр-конкурс по охране труда. Конкурс проводится в целях активизации работы в области обеспечения требований охраны труда, осуществления контроля за их выполнением, соблюдением личным составом структурных подразделений законодательных и иных нормативно-правовых актов по охране труда, организации профилактической работы по предупреждению производственного травматизма, созданию условий безопасной работы личного состава при несении караульной службы, проведении занятий и учений, тушения пожаров и связанных с ними первоочередных аварийно-спасательных работ;

10. В соответствии с приказом МЧС России от 26.10.2017 № 472 «Об утверждении Порядка подготовки личного состава пожарной охраны» в течении учебного года изучается дисциплина «Охрана труда», в объеме 8 часов. Ежеквартально

личный состав сдает зачеты по пройденным темам;

11Обязательные медицинские осмотры проходят все сотрудники, что составляет 100% от общего количества личного состава ПСЧ, подлежащих медицинскому осмотру;

12. В учебном классе ПСЧ созданы уголки охраны туда;

13. Во всех служебных помещениях вывешены инструкции по охране труда;

14. Ежегодно с определенной периодичностью личному составу ПСЧ выдаются сертифицированные средства индивидуальной защиты, боевая одежда пожарного, каска, карабин, защитная обувь пожарного, подшлемник. Учет и выдачу средств индивидуальной защиты производит инженер ПСЧ;

15. Ежегодно, в соответствии с графиком проведения испытаний пожарно-технического вооружения производится испытания пожарно-технического вооружения.

При исследовании причин несчастных случаев, которые произошли с пожарными, было установлено, что большинство составляют организационные причины. Анализ возникновения травмоопасных ситуаций, приводящих к несчастному случаю, также показывает, что технические, технологические, санитарно-гигиенические причины, являются в основном следствием организационных причин, связанных с недостатками в организации работ, обучения, инструктирования, контроля, несоблюдением требований нормативных документов.

Необходимый уровень квалификации пожарного обеспечивается первоначальным обучением (учебный центр, учебное заведение), однако последующее самообучение происходит при выполнении им непосредственной работы по тушению пожаров и проведению аварийно-спасательных работ. Совершенствование систем обучения и ответственности сотрудников за свои неправильные деяния существенно влияет на их поведение. Важно существенно улучшить первоначальную подготовку пожарных в области безопасности труда за счет увеличения времени обучения, применения тренажеров и наглядных пособий для отработки навыков высококвалифицированного и безопасного труда. На данный момент оценивается только травматизм и гибель личного состава, как один из показателей служебной и оперативно тактической деятельности подразделения. Этот показатель, конечно же, не дает полного и объективного представления о состоянии условий и безопасности труда в подразделениях пожарной охраны. Следовательно, важнейшим направлением в области профилактики травматизма является совершенствование организационной работы:

- улучшение качества расследования несчастных случаев;
- улучшение качества анализа травматизма;
- разработка рационализаторской работы на основе анализа травматизма, с целью повышения уровня безопасности труда пожарных и улучшения условий труда;
- разработка рекомендаций и предложений по повышению безопасности труда пожарных;
- совершенствование системы обучения и контроля труда пожарных на основе анализа травматизма, причин несчастных случаев;
- использование методики оценки состояния охраны труда в подразделениях;
- разработка и внедрение автоматизированной информационной системы для эффективного функционирования системы управления охраной труда в пожарной охране;
- формирование социально-психологических условий позволяющих снизить травматизм и профессиональную заболеваемость.

На основе проведенного анализа производственного травматизма, исследований и рекомендаций, разработан перечень организационно-технических мероприятий по охране труда в целях улучшения условий труда и повышения безопасности труда в подразделениях пожарной охраны:

1. замена старых образцов пожарной техники и пожарно-технического вооружения на современные, отвечающие всем требованиям настоящего времени;

2. внедрение систем робототехники с целью обеспечения безопасности сотрудников при проведении разведки места пожара;

3. внедрение систем автоматического контроля и сигнализации уровней опасных и вредных производственных факторов;

4. внедрение и совершенствование технических устройств, обеспечивающих защиту от поражения электрическим током.

5. устройство новых и совершенствование имеющихся средств коллективной защиты от воздействия опасных и вредных производственных факторов;

7. приведение естественного и искусственного освещения служебных помещений к нормам в соответствии с требованиями;

9. приведение зданий, сооружений, помещений к нормам в соответствии с требованиями;

10. расширение, реконструкция и оснащение санитарно-бытовых помещений, помещений для личной гигиены, помещений для обогрева сушки боевой одежды - в соответствие с требованиями;

11. устройство новых и реконструкция имеющихся мест отдыха, помещений и комнат релаксации, психологической разгрузки в соответствие с требованиями;

12. разработка и обеспечение современной сертифицированной боевой одеждой и снаряжением, средств индивидуальной защиты органов дыхания и зрения в непригодной для дыхания среде;

13. Организация более качественного обучения, инструктажа, проверки знаний по охране труда с использованием наглядных пособий и возможности компьютерной техники.

14. Организация кабинетов, уголков, приобретение для них необходимых приборов, наглядных пособий, демонстрационной аппаратуры и т.п., проведение семинаров, конференций.

15. Разработка, издание, приобретение и распространение инструкций по охране труда, других нормативных актов и литературы в области охраны труда.

Данный перечень мероприятий позволяет рационально и целенаправленно планировать работу по охране труда в подразделениях пожарной охраны, улучшить работу по организации охраны труда. Внедрением этих мероприятий можно добиться создания здоровых и безопасных условий труда в подразделениях и как следствие снизить возможность возникновения травмоопасных ситуаций, материальные потери, сохранить жизнь и здоровье пожарных.

Таким образом, на основе проведенного анализа производственного травматизма, исследований и рекомендаций, разрабатывается перечень организационно-технических мероприятий по охране труда в целях улучшения условий труда и повышения безопасности труда в подразделениях пожарной охраны.

Перечень используемой литературы и источников:

1. Российская Федерация. Правительство Российской Федерации. О порядке обучения по охране труда и проверки знания требований охраны труда: Постановление Правительства РФ от 24.12.2021 № 2464 // СПС «КонсультантПлюс».

2. Российская Федерация. Законы. О специальной оценке условий труда: Федер. закон от 28.12.2013 № 426-ФЗ // СПС «КонсультантПлюс».

3. Российская Федерация. Законы. Об обязательном социальном страховании от несчастных случаев на производстве и профессиональных заболеваний: Федер. закон от 24 июля 1998 г. №125-ФЗ (ред. от 08.12.2020) // СПС «КонсультантПлюс».

4. Приказ приказа ГУ МЧС России по Тамбовской области от 10.06.2022 № 555 «О проведении специальной оценки условий труда в ГУ МЧС России по Тамбовской области».

5. Минтруда России. Об утверждении Правил по охране труда в подразделениях пожарной охраны: Приказ Минтруда России от 11.12.2020 № 881н. https://docs.cntd.ru/document/573191712 (Дата обращения: 18.11.2023).

6. МЧС России. Об утверждении Порядка подготовки личного состава пожарной охраны: Приказ МЧС России от 26.10.2017 № 472. https://docs.cntd.ru/document/542610981 (Дата обращения: 18.11.2023).
7. Семенова Е.В. Целесообразность использования виртуально-интерактивного программного комплекса при проведении анализа и оценки риска возникновения чрезвычайных ситуаций на пожаро- и взрывоопасных объектах // Сборник материалов Всероссийской (очно-заочной) научной конференции преподавателей, аспирантов и студентов (Хабаровск, 26-27 декабря 2022г.). [Электронное научное издание: 1 Файл – 19,57 Мб]. – Режим доступа: https://hiik.ru/about_the_university/nauka-i-innovatsii / Ред. кол.: профессор, д.т.н., Кривошеев И.А. и др.; Группа НИРиДО УМО. – Хабаровск: Изд-во ХИИК (филиал) СибГУТИ, 2023. – С. 269-272.
8. Семенова Е.В., Бойков Е.А. Вопросы промышленной безопасности в условиях производственной среды: монография / Е В. Семенова, Е.А. Бойков. – Воронеж: ИПЦ «Научная книга», 2022. – 92 с.

2.11. ИНФОРМАЦИОННО-ПСИХОЛОГИЧЕСКОЕ ПРОТИВОБОРСТВО: ТЕОРЕТИКО-ПРАКТИЧЕСКИЙ АСПЕКТ ПРОБЛЕМЫ

В данной статье автор отмечает, что в настоящее время глобальность современных информационных процессов и отсутствие необходимых знаний и времени у подавляющего большинства людей для составления объективного мнения о событиях и явлениях в мире приводит к упрощению и некритичному восприятию получаемой информации, что создает возможность широко влиять на общественное мнение, преследуя политические интересы.
Ключевые слова: геополитика, геополитические операции (ГО), информация, информационная война (ИВ), информационно-психологическое воздействие (ИПВ), информационное пространство, информационный процесс, психология, психологическая война, теория манипулирования, фейк.

INFORMATION-PSYCHOLOGICAL CONFRONTATION: THEORETICAL AND PRACTICAL ASPECT OF THE PROBLEM

In this article, the author notes that currently the global nature of modern information processes and the lack of necessary knowledge and time for the vast majority of people to form an objective opinion about events and phenomena in the world leads to a simplification and uncritical perception of the information received, which creates the opportunity to widely influence the public opinion, pursuing political interests.
Keywords: geopolitics, geopolitical operations (GO), information, information warfare (IW), information-psychological influence (IPI), information space, information process, psychology, psychological warfare, manipulation theory, fake.

Разрушайте всё хорошее в стане противника, подстрекайте молодёжь против стариков, разжигайте ссоры и столкновения среди граждан вражеской страны, сковывайте волю противника бессмысленными песнями и музыкой, обесценивайте все традиции и богов ваших врагов.

Сунь-цзы

Глобальность современных информационных процессов и отсутствие у подавляющего большинства людей необходимых знаний и времени для составления объективного мнение о событиях и явлениях в мире, ведет к упрощению и некритичному восприятию получаемой информации, что создает возможность широко воздействовать на общественное мнение, преследуя политические интересы.

Необходимо отметить, что неразрывная информационная связь с окружающей действительностью – одно из важнейших условий нормальной жизнедеятельности человека в обществе.

Информация совмещает в себе как созидательно, так и деструктивное воздействие. Определяющим фактором реализации интересов государств на

международной арене становится контроль над потоками информации, результатом чего явилось появление термина «информационная война».

Информационная война представляет собой «комплекс мер, призванных оказать психологическое воздействие, как на отдельных лиц, так и на большие группы людей с целью изменения их настроения, установок и поведения в выгодном для субъекта этого воздействия плане» [8, с. 78-94].

Еще в XIX веке английский исследователь психологической войны П.Г. Уорбертон писал: «Основной задачей в войне является не уничтожение вооруженных сил противника, как это было раньше, а подрыв морального состояния населения вражеской страны в целом до такого уровня, чтобы оно заставило свое правительство пойти на мир. Вооруженное столкновение армий – это лишь одно из средств для достижения этой цели» [8, с. 78-94].

Один из первых случаев применения информационно-психологических воздействия (ИПВ) относится еще к V в. до н.э., когда персидский царь Ксеркс I, пытаясь устрашить эллинов, распространял слухи о гигантских размерах своей армии [1].

Существуют различные концепций, информационно-психологической войны, среди которых можно выделить восемь основных: «управляемый хаос», «сетевая война», «информационно-сетевая война», «операции по достижению эффекта», «преэмптивная война», «геополитическая операция», «стратегия непрямых геополитических действий» и «политическая война».

Остановимся на концепте «геополитической операции» (ГО) изначально предложенной и разработанной российскими исследователями Л.Г. Ивашовыми К.В. Сивковым. ГО рассматривается как новая высшая форма межгосударственного противоборства на глобальном и региональном уровне со своими этапами подготовки и проведения, которая превосходит военные действия по охватываемому пространству, количеству и разнообразию привлекаемых сил и средств.

Цели ГО – ликвидация геополитического противника или смена власти в той или иной стране. Содержание геополитической операции составляют операции и боевые действия группировок вооруженных сил и иррегулярных формирований, тайные операции спецслужб, мероприятия экономической войны, дипломатической и информационной борьбы.

Примерами этих форм действий в межгосударственном противоборстве служат осуществленные Западом восточноевропейские (завершились распадом блока социалистических стран и расширением НАТО на восток), Евро-Азиатская (закончилась дезинтеграцией СССР), Восточно-Азиатская (попытка установления контроля над Ираком и Афганистаном) и Североафриканская – «арабская весна» (смена режимов в странах Магриба) операции.

Так же стоит отметить, что современное информационно-психологическое воздействие (ИПВ) необходимо рассматривать в рамках теории и практики ведения войн четвертого поколения, или стратегии «4GW» – самостоятельного вида воздействия, эффективного оружия, направленного на ослабление психологической устойчивости противника, подавление его морального духа, на возбуждение политической, социальной, экономической активности управляемых масс. Конечной целью такого воздействия являются массовые выступления для свержения политического режима, возбуждение интереса к социально-политическим конструкциям альтернативного характера.

Тем самым, объектами воздействия являются: сознание [5, с. 220-226], воля, чувства населения государства - противника, особенно в периоды выборов, референдумов, кризисных и чрезвычайных ситуаций; лиц принимающие управленческие решения в ключевых сферах жизнедеятельности государства, в том числе в сфере обеспечения безопасности и обороны. Данный тезис подтверждается

массовыми беспорядками, носящими экстремистский и террористический характер, в Республики Казахстан, после которых, председателю Комитета национальной безопасности Казахстана К. Масимову было выдвинуто обвинение в государственной измене [3].

При этом такое воздействие должно быть понятным и доступным для восприятия, совпадать с моделью восприятия окружающего мира. Каждое государство обладает уникальной духовно-психологической системой, которая включает в себя целостную исторически сформированную систему бессознательных установок населения и бессознательную реакцию этого населения на ситуацию, связанную с угрозой для жизни, а также бессознательные инстинкты самосохранения [9, с. 70-75].

Анализ современных тенденций ИПВ дает возможность выделить его основные направления, воздействуя на которые можно добиться изменения культурного кода страны.

Первое направление – *мировоззренческое, воздействие, на которое осуществляется путём массированного внедрения в сознание людей множества ложных стереотипов восприятия и мышления.*

Второе, хронологическое – *представляет собой выхолащивание исторических ориентиров и их замена удобными для субъектов воздействия фактами или мифами.*

Третьим направлением является фактологическое – *т.е. формирование отношения людей к тем или иным событиям, путем субъективной подачи информации, исключающей возможность существования другой, противоположной оценки.*

Принимая во внимания ситуацию в информационном пространстве, сложившуюся на фоне проведения специальной военной операции на Украине, стоит отдельно остановится на таком явлении в западной культуре, как русофобия, которая активно используется в информационно-психологической войне западными странами, как в отношении населения своих государств, так и для дезорганизации населения России.

Русофобию необходимо понимать не просто как проявление негативных чувств в отношении России и русской культуры, но как довольно целостную идеологию, то есть особый комплекс идей и концепций, имеющий свою структуру, свою систему понятий и свою историю генезиса и развития в западной культуре, а также свои типичные проявления [2, с. 251-252].

Субъектами информационно-психологической войны являются государства, имеющие в отношении объекта воздействия свои геополитические интересы, как правило связанные с контролем территории и беспрепятственном доступе к природным ресурсам. Непосредственные мероприятия по оказанию воздействия реализуются внешнеполитическими ведомствами, спецслужбы, информационно-пропагандистскими структурами, транснациональными коммерческими компаниями, подконтрольными международными организациями и другими структурами, имеющими возможности оказывать влияние на большую аудиторию.

Основными принципами организации и проведения информационно-психологической войны являются: принцип асимметричности конфликта; принцип маневренности; «войны без правил» и «войны всех против всех»; принцип хаоса; принцип спецэффектов, принцип боевой стаи; принцип «победы без управления».

Современное оружие информационно-психологической войны представлено использовать телевидение, радио, социальные сети, компьютерные игры, киноиндустрия, литература, СМИ, Интернет, мобильная связь, глобальная навигация и т.д.

Исследую историю технологии информационно-психологической войны, можно сделать вывод о существовании широкого спектра примеров осуществления влияния, который варьируется от распространения литературы, листовок, до создания и

поддержки организаций, лоббирующих цели воздействующего субъекта, в том числе в виртуальном пространстве. Так, немецкие издания, в годы Первой мировой войны (29.07.1914-11.11.1918), публиковали газету на французском языке, где в числе прочего печатали имена захваченных в плен французских солдат. В тоже время, советское правительство, переименовали населенные пункты, имеющие немецкие названия, в том числе столицу Российской империи Санкт-Петербурга в Петроград, также активно велась смена немецких фамилий на русские.

В XX веке велась активная популяризация подвигов героев, которая велась не только путем публикации в печатных изданиях и трансляциях в теле- и радиоэфире, но размещение портретов героев на товарах общего потребления (папиросных упаковках, конфетных обертках).

Некоторые исследователи к акциям информационно-психологической войны относят принятие нормативно-правовых актов, так советские декреты «О мире», «О земле», были обращены не столько к правительству, сколько непосредственно народным массам и имели ярко выраженный пропагандистский характер. Существенную роль в информационно-психологической войне играют лидеры мнений. Так И.В. Сталин, после нападения фашисткой Германии на Советский Союз произнес речь, в которой обратился не традиционным «товарищи», а «братья и сестры».

На сегодняшний день, в науке насчитывается более 60 методов ИПВ, как правило применение тех или иных методов зависит от цели воздействия, аудитории, ее культурно-исторических взглядов и мировоззрений, и возможностей средств манипуляции.

Преимущественно, информационно-психологическая война осуществляется по двум основным формам, которые могут носить как конструктивный, так и деструктивный характер.

Первая форма пропаганда. Термин «пропаганда» произошел от латинского «propaganda» и означает «распространение». В науке пропаганда активно стала исследоваться лишь с XIX века. Можно выделить две основные школы ученых, которые стали рассматривать это понятие: функциональное направление и критическое (Франкфуртская школа) [4].

Представителей функционального направления в политических науках, такие как Гарольд Лассуэлл (1902-1978), Уолтер Липпманн (1889-1974), Карл Ховланд (1912-1961), Джозеф Лиллекер (1915-1990), заложили теоретические основы понимания пропаганды и выделили основные методы и способы ее проведения.

Так, Дж. Лиллекер считал, что пропаганда – это «коммуникация, которая была разработана одной социальной группой с целью – повлиять на мнение, установки и поведение других. В пропаганде часто используют символизм и риторику, она обращена к эмоциональному и иррациональному аспектам нашего восприятия» [6].

В свою очередь, Г. Лассуэлл сформулировал формулу, задающей определенный формат описания коммуникации: «Кто сообщает, что сообщает, по каким каналам, кому и с какими эффектами?». Также, ученый, утверждает, что общество состоит из разных групп и слоев, чьи интересы далеко не одинаковы. Лассуэлл показывает, что степень эффективности пропаганды в немалой степени определяется способностью учесть эти особенности и донести до представителей специфических групп именно то, что может повлиять на их поведение [6].

В своей книге У. Липпманна ввел в научную сферу понятия «agendasetting» (создание повестки дня), то есть тех событий, которые после внесения в общественное внимание подлежат обсуждению населением. У. Липпманн писал о том, что масс-медиа служат связующим звеном между реальными событиями и образами в сознании людей.

Рассматривая подходы Франкфуртской школы, отдельно стоит остановиться на работах ведущих представителей Франкуртского института социальных исследований

– Макса Хоркхаймера (1895-1973), Теодора Адорно (1903-1969), Герберта Маркузе (1898-1979), а также Эриха Зелигманна Фромма (1900-1980).

По мнению Т. Адорно и М. Хоркхаймера, массовое производство культурных форм предполагает унификацию индивидуальных особенностей. Ученые полагают, что аудитория есть некая однородная масса, которой предлагаются заранее апробированные материалы. Другим важным обстоятельством, на которое обращают внимание Т. Адорно и М. Хоркхаймера, является акцент на формирование у аудитории качеств пассивности и конформизма.

Э. Фромм, рассуждая о пропаганде, в своей книге «Бегства от свободы», говорит, что во многих случаях граждане Германии, ничего не имеющие с нацизмом, защищают его от критики иностранцев, потому что расценивают эту критику как нападки на их страну. Важнейшая аксиома политической пропаганды [10]. Любые нападки на Германию как таковую, любая пропаганда, порочащая немцев, только усиливают лояльность тех, кто еще не вполне отождествляет себя с нацистской системой. Эта проблема не может быть решена даже самой умной и искусной пропагандой.

Также, Э. Фромм выделил определенный алгоритм пропаганды, включающий следующие этапы: первый, создание определенного типа поведения; второй, трансформация этого типа поведения в естественную привычку, с помощью пропаганды; третий, фиксация этой привычки через тиражируемую индустрией культуры продукцию [10].

Детально, данный алгоритм был воплощен в технологии «Окна Овертона», которая была названа в честь американского ученого и психолога Джозефа Овертона (1960-2003), который, изучил методику дегуманизации человека и объяснил, как пошагово переформировывать человеческое восприятие к неприемлемому, отвратительному и постыдному в нормальное и даже престижное, то есть постепенное уничтожение моральных принципов человека. При этом, у объекта воздействия формируется иллюзия, что он самостоятельно делают выбор и принимают осознанное решение.

Второй формой ведения информационно-психологической войны является манипуляция. Термин «манипуляция» произошел от латинского слова *«manipulare»* и означает *«управлять»*.

В теории манипуляции выделяют первичную и вторичную. Первичная манипуляция – целенаправленный процесс, скрытого управления волей и чувствами объекта управления. Вторичная манипуляция – прежде всего это результат первичной манипуляции, который может распространяться самими жертвами манипуляции. Яркий пример вторичной манипуляции – посты в социальных сетях в Интернете людей, которые были подвержены манипуляции, и теперь эту информацию распространяют дальше.

Как, уже отмечалось, СМИ являются ключевым инструментом влияния. Существуют трактовки методов манипулирования в средствах массовой информации, среди которых можно выделить: распространение «фейков», фабрикация фактов, подмена смысла слова и понятия, сенсационность, внушение, перенос частного к общему, фрагментация.

Исходя их анализа информационно-психологической войны, осуществляемой в отношении России, можно утверждать, что она осуществляется с помощью значительных сил и средств геополитических соперников.

Тем самым, факторами устойчивости государства, в складывающихся условиях, являются: идейно-ценностная сфера общества; высокий уровень социально-экономической, межэтнической и межконфессиональной стабильности; степень поддержки обществом политического режима; стабильное функционирование системы

государственного управления; инфраструктуры жизнеобеспечения; военной организации; состояние международных отношений.

Перечень использованной литературы и источников:

1. Волковский Н.Л. История информационных войн. В 2-х томах. Т. 1 (с древнейших времен по XIX век) / под ред. И. Петрова. – СПб.: Полигон, 2003. – 502 с.
2. Гройс Б. Россия как подсознание Запада // Гройс Б. Утопия и обмен: Сборник статей. – Москва: Издательство «Знак», 1993. – С. 251-252.
3. Доклад по данным следствия, председателю КНБ Казахстана неоднократно докладывалось о деятельности террористических и экстремистских организациях, а также их пособниках в крупных городах республики, при этом конкретных действий, по предупреждению создающейся угрозы приняты не были. [Электронный ресурс]. – URL: htpps://www.iz.ru/ (дата обращения: 15.09.2023).
4. Иванов А.А. Коммуникативное пространство войны: пропаганда и общественные настроения: Учебно-методическое пособие / А.А. Иванов. – СПб.: ООО «Сфера», 2017. – 72с.
5. Кихтан В.В. Исследование процессов манипулирования сознанием в современных средствах массовой информации / В.В. Кихтан // Вестник Волжского университета им. В.Н. Татищева. – 2018. - №2. – Т2. – С. 220-226.
6. Лассуэлл Г.Д Техника пропаганды в мировой войне / перевод с англ. / Г.Д. Лассуэлл; РАН. ИНИОН. Центр социал. научн. - информ. исследований, Отд. политической науки, Отд. социологии и социальной психологии; сост. и переводчик В.Г. Николаев; отв. ред. Д.В. Ефременко; вступ. статья Д.В. Ефременко, И.К. Богомолова. – Саратов: ООО «Амирит», 2021. – 237 с.
7. Лиллекер. Д. Политическая коммуникация. Ключевые концепты / Д. Лиллекер; пер. с англ. С.И Остенек. – Харьков: «Гуманитарный центр», 2010. – 300 с.
8. Синчук Ю.В. Информационные структуры армий ведущих зарубежных государств / Ю.В. Синчук // Вестник Московского государственного лингвистического университета. Общественные науки. 2017. – № 787. – С. 78–94.
9. Ситникова И.В. Информационно-психологическое воздействие как практика ведения войн четвертого поколения / И.В. Ситникова, А.А. Поляков // Власть. – 2018. - №7. – С. 70-75.
10. Фромм Э. Бегство от свободы / Э. Фромм; общ. ред. П.С. Гуревича; пер. с англ. Г.Ф. Швейника. – Москва: Флинта: МПСИ: Прогресс, 2006. – 248 с.

2.12. КИБЕРБЕЗОПАСНОСТЬ – ВНУТРЕНИИ И ВНЕШНИЕ УГРОЗЫ, СВЯЗАННЫЕ С ИСПОЛЬЗОВАНИЕМ КОМПЬЮТЕРНЫХ ТЕХНОЛОГИЙ

В статье рассматриваются опасности и угрозы компьютерным системам, а также обеспечение кибербезопасности с помощью компьютерных технологий. Упреждающее, комплексное использование системы мер и модернизация систем защиты обеспечат защиту от киберугроз.

Ключевые слова: внутренние и внешние угрозы**,** кибератака, кибербезопасность, кибертерроризм, киберугроза, кибершпионаж, культура кибербезопасности, проактивные меры кибербезопасности, фишинг.

CYBERSECURITY AND INTERNAL AND EXTERNAL THREATS RELATED TO THE USE OF COMPUTER TECHNOLOGY

The article discusses the dangers and threats to computer systems, as well as ensuring cybersecurity using computer technology. Proactive, comprehensive use of a system of measures and modernization of protection systems will ensure protection against cyber threats.

Key words: internal and external threats, cyber-attack, cyber security, cyber terrorism, cyber threat, cyber espionage, cyber security culture, proactive cyber security measures, phishing.

Современный мир не может существовать без компьютерных технологий. Они используются в банковской сфере, здравоохранении, образовании, производстве и других отраслях экономики. Однако, с развитием информационных технологий возникла необходимость в защите компьютерных систем от вредоносных атак. Нарушение работы компьютерных систем может привести к серьезным последствиям, таким как утечка конфиденциальной информации, потеря денежных средств и негативные последствия для бизнеса. Поэтому кибербезопасность становится одной из главных задач компаний и государственных учреждений.

Существует множество видов киберугроз, которые могут быть использованы для атаки на компьютерные системы. Они включают в себя вирусы, трояны, фишинг, а также кибершпионаж и кибертерроризм. Каждый из этих видов угроз имеет свои характеристики и мотивации для атаки на компьютерную систему, более подробно, с ними можно ознакомиться в таблице.

Вид киберугрозы	Описание	Последствия
Вирусы	Вредоносные программы, которые распространяются по компьютерным сетям	Удаление, модификация или кража данных, снижение производительности компьютерной системы, блокирование работы компьютерной системы
Троянские программы	Вредоносные программы, которые скрываются под обычными программами	Удаление, модификация или кража данных, удаленный доступ к компьютерной системе
Фишинг	Мошенничество, направленное на получение личной информации пользователей	Кража личных данных, использование данных для мошеннических целей
Кибершпионаж	Нелегальный сбор информации об объекте	Получение конфиденциальных данных, нарушение конкурентной борьбы, нарушение государственной безопасности
Кибертерроризм	Нанесение ущерба объектам	Нарушение работы системы, потеря жизней

Как видно из таблицы, существует несколько основных видов киберугроз, каждый из которых имеет свои характеристики и последствия. Они могут привести к удалению, модификации или краже данных, снижению производительности компьютерной системы, блокированию работы компьютерной системы, краже личных данных, использованию данных для мошеннических целей, получению конфиденциальных данных, нарушению конкурентной борьбы, нарушению государственной безопасности и даже потере жизней.

Для защиты компьютерных систем от киберугроз необходимо использовать комплексную систему мер, которая включает в себя технические и организационные меры. К техническим мерам относятся:

1. Использование антивирусного ПО, которое может обнаруживать и удалять вирусы и другие вредоносные программы.

2. Использование брандмауэров, которые могут блокировать нежелательный трафик и защищать компьютерную систему от внешних атак.

3. Использование систем обнаружения вторжений, которые могут обнаруживать необычную активность в компьютерной системе и предотвращать взломы и другие атаки.

Также существуют и организационные меры по защите компьютерных систем и информации. Они являются одним из важных компонентов комплексной системы мер по обеспечению кибербезопасности. Эти меры включают в себя политики, процедуры и правила, которые регулируют использование информации и компьютерных систем внутри организации. Организационные меры направлены на снижение рисков, связанных с нарушением информационной безопасности, и на создание более безопасной рабочей среды для сотрудников.

Организационные меры включают в себя:

а) Установку политик безопасности, которые определяют правила использования компьютерной системы, требования к паролям, обработку конфиденциальной информации и т.д.

b) Проведение обучения сотрудников в области кибербезопасности, чтобы они знали, как правильно использовать компьютерную систему и как определить потенциальные угрозы.

c) Создание культуры безопасности, которая обучает сотрудников сохранять безопасность своей компьютерной системы и помогает предотвращать потенциальные угрозы.

Поэтому, для того чтобы обеспечить полную защиту от киберугроз, необходимо использовать комплексную систему мер, включающую в себя как технические, так и организационные меры, а также обеспечивать постоянное обновление и модернизацию системы защиты для того, чтобы она соответствовала новым требованиям и вызовам. Также стоит немного подробнее остановиться на теме последствий разных видов киберугроз, которые могут причинить серьёзный ущерб компаниям или организациям, поэтому необходимость защиты от кибератак становится все более актуальной. Последствия киберугроз могут быть катастрофическими для компаний и государственных учреждений. Согласно отчету компании «IBM Security» [1], средний размер ущерба от кибератаки составляет 3,86 миллиона долларов США или же почти 3 млрд. рублей. Последствия атак могут включать в себя утечку конфиденциальной информации, потерю денежных средств, нарушение работы компьютерной системы и другие серьезные последствия.

Кибербезопасность является проблемой не только для отдельных компаний и государственных учреждений, но и для всего мира. Согласно отчету компании «McAfee» [2], в 2020 году было зарегистрировано 419 миллионов новых вирусов, что на 11% больше, чем в 2019 году. Одной из наиболее серьезных киберугроз является рост числа атак типа «*рыболовные сети*» (phishing) и «*спам-атак*» (spamming). Также можно отметить, что в 2021 году было зарегистрировано рекордное количество кибератак. Согласно данным компании «SonicWall» [3], число кибератак в первом полугодии 2021 года выросло на 40% по сравнению с аналогичным периодом прошлого года. Специалисты также отмечают, что пандемия коронавируса стала одной из причин увеличения количества кибератак. За период пандемии многие компании перешли на удаленную работу, что создало новые уязвимости в системах безопасности и стало причиной увеличения количества кибератак. Прогнозы на ближайшее будущее также неутешительны. Как сообщает компания «Cybersecurity Ventures» [4], в 2023 году ожидается, что затраты на борьбу с киберугрозами достигнут 10,5 триллионов долларов, что в 4 раза больше, чем в 2015 году. Кроме того, они прогнозируют, что в 2024 году число кибератак достигнет 11,5 миллиардов в год.

Данные статистики показывают, что киберугрозы являются серьезной угрозой для бизнеса и общества в целом. Проактивное использование мер по обеспечению кибербезопасности становится все более важным, поскольку злоумышленники становятся все более изобретательными и находят новые способы атак.

Защита от киберугроз становится все более сложной задачей, поскольку злоумышленники постоянно совершенствуют свои методы атак. Поэтому важно следить за последними тенденциями в области кибербезопасности и использовать комплексную систему мер для защиты компьютерной системы.

Результаты исследования показывают, что кибербезопасность и угрозы, связанные с использованием компьютерных технологий, являются серьезной проблемой, которая требует внимания и комплексных мер по обеспечению безопасности информации. Существует несколько основных видов киберугроз, каждый из которых может привести к различным последствиям, таким как ущерб компьютерной системе, потере конфиденциальности данных, нарушению целостности данных, недоступности компьютерной системы и т.д. Для защиты от киберугроз необходимо использовать комплексную систему мер, включающую в себя технические

и организационные меры, которые позволят предотвратить ущерб, который может нанести кибератака.

Кроме того, было обнаружено, что число кибератак постоянно растет. В 2020 году было зарегистрировано 419 миллионов новых вирусов, что на 11% больше, чем в 2019 году. В 2021 году число кибератак продолжило расти, причем пандемия коронавируса стала одной из причин увеличения количества кибератак. Прогнозы на ближайшее будущее также неутешительны, поскольку ожидается еще большее увеличение числа киберугроз в мире.

Таким образом, защита от киберугроз является одной из важнейших задач в области информационной безопасности. Для того чтобы обеспечить полную защиту от киберугроз, необходимо использовать комплексную систему мер, включающую в себя как технические, так и организационные меры, а также обеспечивать постоянное обновление и модернизацию системы защиты.

Перечень использованной литературы и источников:

1. IBM Security. 2020 Cost of a Data Breach Report. [Электронный ресурс]. – URL: https://www.ibm.com/security/data-breach (дата обращения: 25.03.2023).
2. McAfee. McAfee Labs Threats Report: November 2020. [Электронный ресурс]. URL: https://www.mcafee.com/blogs/other-blogs/mcafee-labs/mcafee-labs-threats-report-november-2020/ (дата обращения: 25.03.2023).
3. SonicWall. 2021 SonicWall Cyber Threat Report. [Электронный ресурс]. – URL: https://www.sonicwall.com/resources/white-papers/2021-sonicwall-cyber-threat-report/283f84e7-2d1c-4a72-8df0-6c8d01f23e69 (дата обращения: 25.03.2023).
4. Cybersecurity Ventures. Cybersecurity Spending Predictions, 2021-2023. [Электронный ресурс]. – URL: https://cybersecurityventures.com/cybersecurity-market-report/ (дата обращения: 25.03.2023)
5. Митник К., Саймон У. Искусство обмана. Секреты социальной инженерии. – Москва: Альпина Паблишер, 2021. – 384 с.
6. Павлов А.И., Лукичева Е.В., Трусова Ю.А. Кибербезопасность: учебник для студентов вузов. – Москва: Юрайт, 2019. – 292 с.
7. Лебедев И.В. Кибербезопасность и информационные войны. – Москва: МИФИ, 2018. – 168 с.
8. Гончаров С.В., Лукина Т.В. Кибербезопасность: учебник для вузов / С.В. Гончаров, Т.В. Лукина. – СПб.: БХВ-Петербург, 2017. – 416 с.

2.13. ИНФОРМАЦИОННАЯ БЕЗОПАСНОСТЬ КАК ОСНОВНОЕ НАПРАВЛЕНИЕ РЕАЛИЗАЦИИ НАЦИОНАЛЬНОГО ПРОЕКТА РОССИИ «ЦИФРОВАЯ ЭКОНОМИКА»

В данной работке автор рассматривает аспект информационной безопасности как основное направление в реализации в России Национального проекта «Цифровая экономика»

Ключевые слова: защита информации, информация, информационная безопасность (ИБ), информационная политика государства, национальный проект «Цифровая экономика».

INFORMATION SECURITY AS THE MAIN DIRECTION OF THE IMPLEMENTATION OF THE NATIONAL PROJECT OF RUSSIA "DIGITAL ECONOMY"

In this paper, the author considers the aspect of information security as the main direction in the implementation of the National Digital Economy Project in Russi.

Keywords: information protection, information, information security (IS), information policy of the state, national project "Digital Economy".

Информационная сфера сегодня глубоко интегрирована во все сферы производства и общественной жизни. На государственном уровне обеспечение информационной безопасности признано одной из концептуальных основ ее дальнейшего развития. Стратегия обеспечения информационной безопасности в Российской Федерации является одним из ключевых направлений реализации концепции цифровизации экономики страны [1].

В таких условиях особое значение приобретает формирование эффективной государственной информационной политики, основанной на инновационных научных исследованиях явлений информационной сферы. При этом во главу угла ставится проблема обеспечения должного уровня защиты информации от внешних посягательств и не законного использования.

Одним из важнейших шагов в систематическом изучении информационной безопасности (ИБ) является углубленный анализ общей структуры ее поддержки.

Назначение и детализация компонентов для обеспечения ИБ по разным причинам должны помочь понять соответствующие базовые параметры, лежащие в основе сформирования комплекса адекватных мер государственного и негосударственного характера, направленных на поддержание оптимального развития информационных систем Российской Федерации на пути её интеграции в глобальное информационное пространство.

ИБ - одна из важнейших составляющих национальной безопасности страны, обеспечение которой через последовательную реализацию четко сформулированной национальной информационной стратегии внесло бы существенный вклад в успех решения политических, военно-политических, военных, социальных, экономических и других проблем в деятельности государственной власти.

Таким образом, реализация эффективной информационной политики может оказать существенное влияние не только на решение задач финансово-экономического характера, но и на успешность борьбы с современными угрозами, как локального, так и глобального характера, повлиять на разрешение внутренних и внешних конфликтов [3, с. 382].

В целях реализации приоритетных задач, направленных на обеспечение ИБ создаётся соответствующая правовая основа. Важное значение имеет, в частности, приказ от 28.12.2020 № 780 «Об определении угроз устойчивости, безопасности и целостности функционирования на территории Российской Федерации сети Интернет и сети связи общего пользования» раскрывает угрозы устойчивости, безопасности и целостности функционирования на территории Российской Федерации сети Интернет и сети связи общего пользования [2].

Современное состояние глобальной ИБ, связано с новыми имеет, в частности, требующими поиска эффективных средств и методов борьбы с ними. Интегрирование технологий повсеместной безопасности позволит заказчикам и поставщикам услуг использовать преимущества обще-ориентированной защиты, поскольку именно такой тип защиты наиболее актуален для противодействия современному динамично развивающемуся спектру угроз. Только в случае введения глобальных мер многоуровневой защиты можно без лишних рисков использовать возможности, которые предоставляет цифровая экономика и всеобъемлющий интернет. Особое внимание следует уделить таким вредоносным программам, как руткиты, которые значительно опаснее, чем обычные вирусы.

Существуют различные методы и способы обеспечения ИБ. Главная задача обеспечения ИБ в стране может быть реализована путем использования всех доступных методов и мер для защиты информационных потребностей общества и самого государства. Организационные объединения государственных органов участвуют в государственном обеспечении информационной безопасности на основании правовых и административных актов.

Поэтому важнейшей предпосылкой для обоснования методов, форм и механизмов их реализации является абсолютное верховенство закона во всех сферах деятельности, в том числе и в политической. Каждый субъект информационного процесса должен иметь соответствующую правовую осведомленность, быть законопослушным, хорошо понимать последствия своих действий для других

субъектов и степень ответственности в случае нарушения его жизненно важных интересов.

Это имеет принципиальное значение, поскольку использование определенных форм и методов зависит от того, являются ли угрозы результатом непреднамеренных или преднамеренных действий субъектов информационного процесса [5, с. 342].

Распространенными методами анализа состояния ИБ являются методы исследования причинно-следственных связей. С помощью этих методов обнаруживаются причинно-следственные связи между угрозами, рисками, вызовами и опасностью. Поиск и выявление причин, которые стали источником угрозы и привели к актуализации определенных факторов риска, лежит в основе разработки мер по их нейтрализации и противодействию.

Среди этих методов установления причинно-следственных связей можно упомянуть следующие: метод подобия, метод различия, метод сообщения о сходствах и различиях, метод изменений, сопровождающий метод остатков.

Следовательно, управление ИБ должно основываться на принципах законности, доступности, конфиденциальности и целостности информации [4, с. 48].

Таким образом, ведя речь о методах защиты информации, нельзя забывать о том, что отождествление ИБ с обеспечением безопасности компьютерных систем является лишь концептуальным недостатком. Важное значение, на наш взгляд, имеет учет так называемого «человеческого фактора», исключить который в работе с информацией не представляется возможным. Современные исследования говорят об отсутствии реальной возможности создания абсолютно надежной системы защиты информации, поскольку, как было отмечено выше, информационные угрозы и опасности являются атрибутивными компонентами системы защиты информации, т.е. их существование и реализация, а также отрицательные последствия являются естественной частью системы защиты информации. Они позволяют нам признать недостатки системы управления информационной безопасностью и в то же время служат стимулом к ее совершенствованию.

Перечень использованной литературы и источников:

1. Российская Федерация. Президент Российской Федерации. О Стратегии национальной безопасности Российской Федерации: Указ Президента РФ от 02.07.2021 № 400 // СПС «KREMLIN.ru».

2. Российская Федерация. МВД России. Об определении угроз устойчивости, безопасности и целостности функционирования на территории Российской Федерации сети Интернет и сети связи общего пользования: Приказ от 28.12.2020 № 780 // СПС «КонсультантПлюс».

3. Афанасьева Д.В., Абидарова А.А., Плахина Е.А. Обеспечение безопасности автоматизированных систем при взаимодействии с сетью интернет // Известия Тульского государственного университета. Технические науки. – Тула: Изд-во ТулГУ. – 2019. Вып. 12. – С. 382-385.

4. Абидарова А.А. Современные проблемы в информационной безопасности / А.А. Абидарова // Интеграция науки, общества, производства и промышленности: проблемы и перспективы: Сборник статей по итогам Международной научно-практической конференции (Омск, 4.11.2021 г.). – Стерлитамак: АМИ. – С. 48-50.

5. Плахина Е.А. К вопросу об информационной безопасности в сети интернет / Е.А. Плахина // Известия Тульского государственного университета. Технические науки. – Тула: Изд-во ТулГУ. – 2020. - Вып. 12. –С. 342-345.

6. Проскуряков Н.Е., Яковлев Б.С. Определение параметров автоматизированного процесса резервного копирования цифровых данных типографий и издательств без использования внешних сетевых технологий / Н.Е. Проскуряков, Б.С. Яковлева // Динамика систем, механизмов и машин. – 2018. Т. - 6. № 2. – С. 50-57.

ГЛАВА 3.
КАДРЫ ДЛЯ РАЗВИТИЯ ЦИФРОВИЗАЦИИ

3.1 ПОДГОТОВКА КАДРОВ ДЛЯ РАЗВИТИЯ ЦИФРОВОЙ ЭКОНОМИКИ

Представленное исследование обобщает и отражает тенденции развития общества в условиях цифровой экономики. Основной акцент в работе сделан на кадровом потенциале обеспечивающим ее развитие. Государственная политика определяет данный аспект как приоритетный и входящий в федеральный национальный проект, предусматривающий существенное финансирование на основе реализации дорожной карты. Образование и кадры в Программе «Цифровая экономика Российской Федерации» отнесены к одному из основных институтов, в формате которых создается среда для планомерного и всестороннего развития цифровой экономики. В Программе определены основные цели и направления, касающиеся кадров и образования: создание ключевых условий для подготовки кадров цифровой экономики; совершенствование системы образования, которая должна обеспечивать цифровую экономику компетентными кадрами; рынок труда, который должен опираться на требования цифровой экономики. В работе рассмотрены кадровые проблемы и изменения на рынке труда, возникающие в связи с развитием цифровой экономики.
Ключевые слова: национальная экономика данных, образование, подготовка кадров, цифровая экономика.

TRAINING OF PERSONNEL FOR THE DEVELOPMENT OF THE DIGITAL ECONOMY

The presented research summarizes and reflects the trends in the development of society in the digital economy. The main focus of the work is on the human resources that ensure its development. The State policy defines this aspect as a priority and included in the federal national project, which provides substantial funding based on the implementation of the roadmap. Education and personnel in the Digital Economy of the Russian Federation Program are classified as one of the main institutions in the format of which an environment is created for the systematic and comprehensive development of the digital economy. The Program defines the main goals and directions related to personnel and education: creating key conditions for training digital economy personnel; improving the education system, which should provide the digital economy with competent personnel; the labor market, which should be based on the requirements of the digital economy. The paper considers personnel problems and changes in the labor market, arising in connection with the development of the digital economy.
Keywords: national data economy, education, training, digital economy.

Введение. Формируемые в результате модернизации экономики «большие данные», наряду с технологиями их анализа, становятся одним из ведущих активов государства, бизнеса и гражданского общества. Разработка национальных программ развития экономики нового поколения, включающая вопросы развития и внедрения технологий, анализа «больших данных» и прогнозирования, внедрения новых способов управления, становится задачей стратегической важности не только в контексте социально-экономического благополучия государств, но и как условие сохранения суверенитета на фоне глобализации и реализации программ цифрового развития другими участниками мирового рынка. В результате анализа концепций цифровой экономики, которые в настоящее время разрабатываются экономистами в России, можно выделить работы В.М. Кулькова, Л.В. Лапидус, Т.Н. Юдиной, Е.Н. Ведута, Т.Н. Джакубова и других.

Понятие «цифровой экономики» в первую очередь связано с зарождением четвертого технологического уклада и на сегодняшний день не имеет общепринятой международной трактовки, что послужило поводом для уточнения термина «цифровая экономика» на правительственном уровне рядом стран. Правовое регулирование цифровизации экономики в России и за рубежом осуществляется на основании

разработанных программ цифровой экономики. Таким образом, можно заключить, что необходимо уточнение понятий на нормативно-правовом уровне в различных странах мира. Рассмотрим определения цифровой экономики, данные национальными правительствами ряда стран и международными организациями (См. Табл. 1).

Таблица 1 – Определения цифровой экономики, утвержденные на правительственном уровне в ряде стран мира

№ п/п	Учреждение	Определение
1	Правительство Австралии	«Глобальная сеть экономических и социальных видов деятельности, которые поддерживаются благодаря таким платформам, как интернет, а также мобильные и сенсорные сети»
2	BCS, Велико-британия	«Ведение бизнеса на рынках, опирающихся на интернет и/или Всемирную паутину»
3	ОЭСР	«Рынки на основе цифровых технологий, которые облегчают торговлю товарами и услугами с помощью электронной коммерции в Интернете»
4	Правительство Великобритании	«Производство цифрового оборудования, издательская деятельность, медийное производство и программирование»
5	Всемирный банк	«Система экономических, социальных и культурных отношений, основанных на использовании цифровых информационно-коммуникационных технологий»
6	Правительство РФ	«Деятельность, в которой ключевыми факторами производства являются данные, представленные в цифровом виде, а их обработка и использование в больших объемах, в том числе непосредственно в момент их образования, позволяют по сравнению с традиционными формами хозяйствования существенно повысить эффективность, качество и производительность в различных видах производства, при хранении, продаже, доставке и потреблении товаров и услуг»

*Источник: UK Digital Strategy 2017 // Department for Digital, Culture Media & Sport. – 1 March 2017. – Electronic text data. – Mode of access: https://www.gov. uk/government/publications/uk-digital-strategy/ukdigitalstrategy

При сопоставлении программ по цифровизации экономики разных стран нами были сделаны следующие выводы: все рассматриваемые страны предполагают введение цифровой экономики путем развития инновационных центров и инвестирования в научные проекты. Также в ходе анализа было выявлено, что все страны признают, что неотъемлемой частью перехода к цифровой экономике являются решения по расширению интернет-коммуникации, направленные на обеспечение доступа к всемирной сети наибольшего количества населения и улучшения качества такой связи. При этом, наиболее важным направлением является цифровизация государственных органов, это, прежде всего, адаптация нормативной базы для перехода на Цифровую экономику, а также автоматизация процессов с целью сократить бюрократию и создание максимальной прозрачности. Особое внимание уделяется развитию и поддержки технологических стартапов, малого и среднего бизнеса.

Исследовательская часть. В целях управления развитием цифровой экономики РФ определены цели и задачи в рамках 5 базовых направлений развития цифровой экономики. К базовым направлениям относятся нормативное регулирование, кадры и образование, формирование исследовательских компетенций и технических заделов, информационная инфраструктура и информационная безопасность.

В соответствии со Стратегией развития информационного общества в Российской Федерации предполагается организовать системное развитие и внедрение цифровых технологий во всех областях жизни: в экономике, предпринимательстве, социальной сфере, а также в государственном управлении. Таким образом, программа «Цифровая экономика Российской Федерации», утвержденная распоряжением Правительства РФ от 28.07.2017 № 1632-р, должна стать основой для развития системы государственного управления, экономики, бизнеса, социальной сферы, всего общества [2, стр. 108].

Правительство РФ составило планы мероприятий (дорожные карты) по четырем направлениям программы «Цифровая экономика Российской Федерации»: «Нормативное регулирование», «Формирование исследовательских компетенций и

технологических заделов», «Информационная инфраструктура», «Информационная безопасность». Кроме указанных направлений программы начали реализовываться новые направления в сфере здравоохранения, создания «умных городов», государственного управления, искусственного интеллекта.

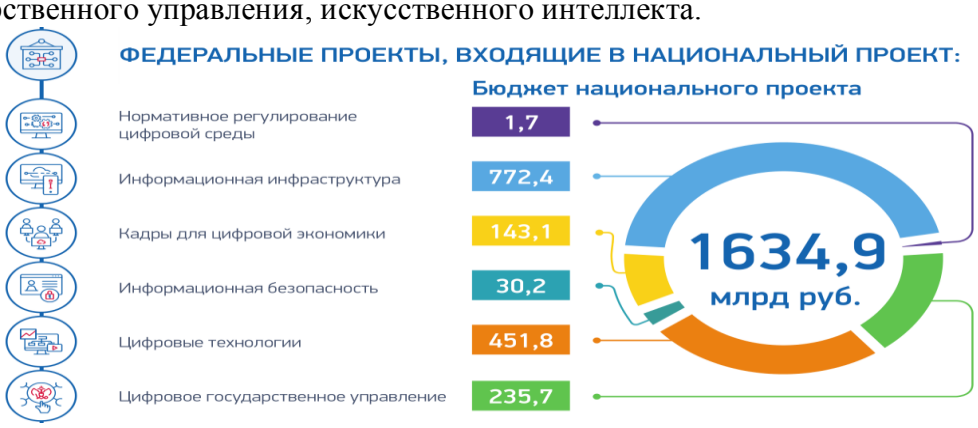


Рисунок 1 - Расходы на федеральные проекты, входящие в национальный проект «Цифровая экономика РФ» на 2018-2024 г, млрд. рублей
***Источник**: Программа "Цифровая экономика Российской Федерации".

До 2020 г. на реализацию дорожных карт по четырем направлениям программы «Цифровая экономика Российской Федерации» планируется израсходовать свыше 521 млрд руб., из которых около 171,2 млрд. руб. будет выделено из бюджета страны, а внебюджетное финансирование составит около 350 млрд. руб. (См. Табл. 2)

Таблица 2 - Финансирование программы «Цифровая экономика Российской Федерации на 2018-2020 г.», млрд. руб.
***Источник**: Правительство Российской Федерации. http://government.ru/

Направления программы «Цифровая экономика Российской Федерации»	Источники финансирования за период с 2018 по 2020 г.	
	из бюджета	внебюджетные средства
Информационная инфраструктура	100	336
Информационная безопасность	22,3	11,7
Формирование исследовательских компетенций и технологических заделов	48	2
Нормативное регулирование	0,9	0,3
Итого	171,2	350

Финансирование национальной программы «Цифровая экономика» в 2023 году было в объеме 129,3 млрд. рублей, что на 35,6% меньше, чем в 2022 году, говорится в пояснительной записке к проекту бюджета, внесенному в Госдуму. На 2024 год финансирование нацпрограммы заложено в размере 126,9 млрд. рублей.[3]

Центрами компетенции являются компании «Росатом» и «Ростех», а курирует данное направление Минкомсвязи России. В процессе его реализации происходит цифровая трансформация секторов российской экономики и отдельных ее субъектов. В частности, в рамках нацпроекта на портале госуслуг было запущено семь суперсервисов: «Поступление в вуз онлайн», «Социальная поддержка онлайн», «Цифровое исполнительное производство», «Трудовые отношения онлайн», «Оформление европротокола онлайн», «Пенсия онлайн» и «Онлайн помощь при инвалидности». [4] А также будет формироваться спрос со стороны субъектов

экономики на продукцию российского происхождения в области «сквозных» технологий, в частности, анализ больших данных, блокчейн, квантовое вычисление, искусственный интеллект.

Цифровые технологии внедряются практически во всех отраслях. Сейчас в проектировании и строительстве государство стимулирует применение информационного моделирования. И там наблюдается нехватке таких специалистов. За короткое время необходимо подготовить и переподготовить по ИТ-профилю огромное число людей из этого сектора экономики.

В последние годы многие государства усилили интерес к развитию экономики данных. Институт статистических исследований и экономики знаний НИИ ВШЭ (г. Москва) проанализировал зарубежные политики управления данными и выявил ключевые тренды и подходы в этой сфере. Остановимся на главных выводах:

- большинство стран признают ключевое значение данных для экономики. Данные на государственном уровне определяются как новый фактор производства (data resources);

- среди общих приоритетов – формирование рынка данных, создание условий для их вовлечения в экономический оборот, переиспользования и извлечения из них максимальной ценности;

- большинство стран (Великобритания, Индия, ЕС) содействуют обмену неперсональными и обезличенными данными, по крайней мере в стратегически и общественно значимых сферах. В Китае обмен данными возможен только в рамках госсектора или в одностороннем порядке от бизнеса к госорганам. В Сингапуре для бизнеса сформирована доверенная система обмена данными B2B с едиными правилами и типовыми договорами;

- все страны стремятся обеспечить защиту персональных данных;

- возможности трансграничных потоков данных в стратегиях стран довольно разные. ЕС запрещает передачу данных своих граждан в любую страну, которая не принимает правила, эквивалентные GDPR, тем самым ЕС подталкивает другие страны принять свой подход к защите данных. Китай полностью запрещает передачу данных за рубеж.

Как комментирует Павел Рудник, заместитель директора Института статистических исследований и экономики знаний НИУ ВШЭ: «В России сейчас ведется проработка нового Национального проекта «Национальная экономика данных», определяются основные контуры политики в этой сфере. В ближайшей перспективе будет необходимо критически оценить эффективность действующих норм, многие «правила игры» придется создать практически с нуля, координируя усилия по формированию институтов и инфраструктуры полноценного рынка данных, который пока находится на ранней стадии развития, как и в большинстве других стран. И здесь есть множество развилок, даже на уровне базовых принципов и подходов к регулированию. Разнообразие применяемых за рубежом моделей управления данными довольно велико – от сугубо протекционистских до довольно либеральных. Государству предстоит найти баланс между такими зачастую противоречивыми ориентирами, как обеспечение защиты персональных данных и суверенитета данных, с одной стороны, и стимулирование вовлечения данных в оборот и извлечения из них максимальной ценности, с другой».

По данным Министерства образования и науки РФ в 2022 году более 117 тыс. человек было принято в вузы на бюджетные места по ИТ специальностям, при этом их реализацию осуществляют более 800 вузов. В 2024 году на обучение планируется принять более 500 тысяч человек. Следует отметить, что активно внедряются и программы дополнительного профессионального образования, идет активная реализация таких проектов как «Цифровые профессии», «Готов к цифре», «CDO»,

позволяющие сформировать необходимые ИТ-компетенции и навыки у руководителей и менеджеров российских компаний.

Основным координатором образовательного процесса с 2019 года является Университет 2035. Он выступает оператором национальных проектов, направленных на подготовку кадров для цифровой экономики и достижения технологического и кадрового суверенитета России. В этом качестве Университет 2035 занимается экспертным отбором лучших на рынке дополнительного образования организаций и программ, принимает заявки на обучение и контролирует его результаты.

В текущем 2024 году Минцифрой РФ начнется реализация новой нацпрограммы «Национальная экономика данных», которая заменит программу «Цифровая экономика», так как он достиг поставленных целей и требует своего дальнейшего развития. Новая программа более глобальна, охватит все регионы и госкорпорации, будет более оперативно ставить и решать текущие вопросы. При этом блок вопросов с развитием кадрового потенциала в ИТ в нацпрограмме «Экономика данных» останется и будет проводится по трем основным направлениям: старшеклассники – курсы программирования, студенты – контрольные цифры приема и цифровые кафедры и корпоративные программы обучения по уровню дополнительного профессионального образования.

На сегодняшний день дефицит кадров в ИТ-отрасли оценивается в полмиллиона человек, а всего в этой сфере сейчас работает около 700 тыс. человек. К 2030 году рынок ИТ услуг по прогнозам экспертов возрастет в 2 раза и что бы ему соответствовать кадровое направление необходимо наращивать, до уровня его сбалансированности которое может наступить не ранее чем 5 лет.

«Заинтересованность на государственном уровне в решение проблемы дефицита ИТ специалистов понятна, но эффективно это можно сделать только в связке с корпоративными программами и самим рынком. Важно найти баланс, а также усиливать привлекательность смежных с ИТ-направлений, например, в радио и микроэлектронике, где подготовка кадров занимает гораздо больше времени», - директор ИТ департамента кадрового агентства «Cornerstone» - Максим Антонов, и с этим мнением нельзя не согласиться.

Рассмотрим политику в области цифровой трансформации, которая проводится на базу ФГБОУ ВО «Сочинский государственный университет». Так сегодня, приоритетной задачей становиться создание комфортной цифровой инфраструктуры, которая позволит на высоком уровне реализовывать образовательные, научно-исследовательские программы и проекты. В процессе ее решения предполагается:

1. Увеличить долю сотрудников Университета, обладающих цифровыми компетенциями.

2. Обеспечить интеграцию информационной системы Университета с ГИС СЦОС.

3. Загрузка сведений в ГИС СЦОС о цифровых зачетных книжках и студенческих билетах обучающихся по образовательным программам высшего образования (бакалавриат, специалитет, магистратура.

4. Увеличить долю ППС, по которым осуществлена выгрузка сведений в ГИС СЦОС в соответствии с API ГИС СЦОС.

5. Обеспечить увеличение доли аспирантов, по которым осуществлена выгрузка сведений в ГИС СЦОС соответствии с API ГИС СЦОС.

6. Увеличить количество электронных сервисов.

7. Увеличить количество оснащенных, учебных помещений, Интернетом.

8. Увеличить мощностей серверной инфраструктуры и систем защиты информации.

Программа «Цифровая экономика Российской Федерации», опираясь на «Стратегию развития информационного общества в Российской Федерации на 2017-

2030 годы», исходит из того, что: «цифровая экономика представляет собой хозяйственную деятельность, ключевым фактором производства в которой являются данные в цифровой форме, и способствует формированию информационного пространства с учетом потребностей населения и общества в получении качественной и достоверной информации, развитию информационной инфраструктуры РФ, созданию и применению российских информационно-телекоммуникационных технологий, а также созданию новой технологической базы для социальной и экономической сферы.» Таким образом, на современном этапе основным активом государства становится человеческий и информационный капитал, человек с высоким уровнем квалификации, умеющий исследовать и анализировать, умеющий создавать и внедрять новое.

В этой связи грядут изменения рынка труда. Одним из механизмов для решения задачи преодоления модели рентной экономики правительство РФ видит в реализации программы «Цифровая экономика». Работа в данном направлении выходит на ключевые позиции, поскольку неразвитость в этом секторе способствует долгосрочным негативным явлениям в условиях, когда мировая экономика развивается в соответствии с новыми трендами и лишает страну возможности быть конкурентоспособной.

Разработка дорожной карты в сфере образования вызывает крайне большой интерес, если не сказать, встревоженность. Управленческие, так и технические кадры, задействованные в инновационном секторе, обладают специфическими качествами и должны проходить особую подготовку, особенно кадры, которые готовятся на «рубеже» бизнеса и государства, например в институтах развития.

Вернувшись к мысли о том, почему проработка дорожной карты является приоритетным направлением в реализации программы цифровой экономики, невозможно не упомянуть взаимосвязь рынка труда и образования.

Прибегнув к авторитетным мнениям о том, что на сегодняшний день происходит на рынке труда в России и мире, Клаус Шваб упоминает в своём широко известном труде: «четвертая промышленная революция создает меньше рабочих мест в новых отраслях, чем предыдущие революции, только 0,6% трудовых ресурсов США заняты в отраслях, не существовавших в начале века; менее 9% новых рабочих мест было создано в 80-ых годах прошлого столетия и 5% новых рабочих мест – в 90-ые годы. Внедрение инноваций в информационно-коммуникационных и других прорывных технологиях содействуют увеличению производительности посредством замены существующих рабочих, а не формирования множества продуктов, которые нуждаются в дополнительном труде для производства». Опираясь на изучение воздействия прорывных технологий на безработицу, экономист Клаус Шваб отмечает: «Полагаясь на результаты данного исследования почти 48% рабочих мест в США подвержены риску автоматизации, по всей вероятности, уже в течение двух ближайших десятилетий, что будет отмечено более широким диапазоном профессий, подверженных разрушению значительно быстрее, чем в результате сдвигов на рынке труда, которые имели место быть в течение предыдущих промышленных революций».

Рост занятости труда будет возрастать в тех сферах и направлениях, где необходим контроль за выполнением сложных технологических процессов и анализом данных, а снизится там, где преобладает тяжелый, неквалифицированный труд». Не стоит забывать о том, что информационная экономика - это не только развитие информационно-коммуникационных технологий, но и формирование совершенно новых бизнес-моделей, эффективность которых выходит на новый уровень. Бизнес приобретает более разветвленную и динамичную форму, в нем нет пошагового руководства к тому, как организовать свою деятельность.

Основываясь на данных «OECD Digital Economy Outlook 2019», можно сделать вывод, что на сегодняшний день экономику и общество лихорадит от цифровой трансформации [9].

На современном этапе в России сложилась некоторая динамика, которая уже достаточно остро ставит вопрос о перспективах рынка труда в эпоху цифровизации. «Шесть лет назад в Сбербанке в бэк- офисе работало 59 тысяч человек. Сегодня работает 12 тысяч. В 2019 году будут работать пять тысяч. А по нашим оценкам, еще через три года будет работать в лучшем случае тысяча», - отмечает Г. Греф [7].

Национальный исследовательский университет «Высшая школа экономики» и «СберБанк» отобрали наиболее перспективные профессии исходя из прогнозных оценок спроса на них в 2023-2024 годах, глобальных трендов научно-технологического развития, динамики изменений российского и мирового рынков труда. Перспективные профессии будущего будут востребованы в сферах здравоохранения, урбанистики, ИТ, кибербезопасности, финансах, дизайне, маркетинге, логистике, юриспруденции, менеджменте в сфере досуга. А также в так называемой сфере «Agile» - это обобщающий термин для ряда подходов и практик по гибкой разработке программного обеспечения и сфера «ESG» - устойчивое развитие, предполагающее повышение экологической, социальной и корпоративной ответственности в работе компаний. Например, в здравоохранении будут востребованы биоинформатики, биоэкономисты, нейрореабилитологи, консультанты по здоровому долголетию, менеджеры индивидуальных медицинских программ.

Заключение. Такие глобальные изменения на рынке труда бросают вызов тому, как будет модернизирован человеческий труд, какие из кадровых ресурсов будут наиболее востребованными, какие модели образования необходимы для новой цифровой экономики. В ближайшее десятилетие будут происходить существенные трансформации на рынках труда, связанные с исчезновением старых и появлением новых профессий, требующих от работника новых навыков. Одним из важнейших условий эффективного развития приоритетных сфер человеческой деятельности в цифровой экономике является создание соответствующей институциональной среды. Основными факторами производства в «завтрашней» экономике становятся человеческий и информационный капиталы, при этом роль основного фактора остается за человеческим капиталом. В ближайшее десятилетие будут происходить существенные трансформации на рынках труда, связанные с исчезновением старых и появлением новых профессий, требующих от работника новых навыков.

Перечень использованной литературы и источников:

1. Российская Федерация. Указы. Доктрина информационной безопасности Российской Федерации. Указ Президента Российской Федерации от 5 декабря 2016 г. №646 «Об утверждении Доктрины информационной безопасности Российской Федерации» // СПС «KREMLIN.ru».
2. Российская Федерация. Правительство Российской Федерации. Об утверждении программы «Цифровая экономика Российской Федерации»: Распоряжение Правительства России от 28 июля 2017 г. №1632-р // СПС «GARANT.ru».
3. Бюджет нацпрограммы «Цифровая экономика» в 2023 году предложено сократить на 35% // СПС «INTERFAX.ru».
4. Путин заявил, что большинство госуслуг через три года должны предоставляться онлайн. ТАСС. Дата обращения: 22/01/2024.
5. Вести Экономика. Путин: цифровая экономика – тема национальной безопасности Российской Федерации. [Электронный ресурс]. – URL: http://www.vestifinance.ru/articles/87680.
6. Виртуальный университет. Почему государство выделяет 2 млрд рублей АСИ на онлайн-обучение. – URL: http://www.forbes.ru/tehnologii/352445-virtualnyy-universitet-pochemu-gosudarstvo-vydelyaet-2-mlrd-rubley-asi-na-onlayn (Дата обращения: 22.01.2024).
7. Индекс развитости информационно-коммуникационных технологий. The Networked Readiness Index (NRI) // TAdvise: [портал]. – 21.07.2016. – URL: http://www.tadviser.ru/index.php/.
8. МГИМО и МФТИ будут вместе готовить управленцев в сфере цифровой экономики. – URL: http://mba.mgimo.ru/news/mgimo-i-mfti-tsifrovaya-ekonomika.
9. Развитие цифровой экономики в России как ключевой фактор экономического роста и повышения качества жизни населения: монография / Андреева Г.Н., Бадальянц С.В., Богатырева Т.Г. и др. – Нижний Новгород: Профессиональная наука, 2018.
10. Российские специалисты назвали профессии будущего. – URL: http://tass.ru/plus-one/4572666.

11. Цифровая Россия: новая реальность. Аналитический отчет экспертной группы Digital. ООО «Мак-Кинзи и Компания СиАйЭс», www.mckinsey.ru.
12. Цифровые навыки населения. Центр статистики и мониторинга информационного общества ИСИЭЗ НИУ ВШЭ. – URL: https://issek.hse.ru/news/207284687.html.

3.2. РАЗРАБОТКА НАБОРОВ БАЗОВЫХ ПОКАЗАТЕЛЕЙ ДЛЯ АВТОМАТИЗИРОВАННОЙ ОЦЕНКИ «ЧЕЛОВЕЧЕСКОГО ФАКТОРА» В СФЕРЕ ОБЕСПЕЧЕНИЯ ИНФОРМАЦИОННОЙ БЕЗОПАСНОСТИ

В представленной статье автором рассматриваются характеристики надежности оператора операционной системы, виды его ошибок и связанные с этим угрозы в сфере обеспечения информационной безопасности (ИБ).
Ключевые слова: автоматизированная оценка «человеческого фактора», анализ психофизиологического состояния, защита информации (ЗИ), информационная безопасность (ИБ), информационно-психологическая безопасность (ИПБ), информационно-психологическое воздействие (ИПВ), оператор автоматизированных систем (АС).

DEVELOPMENT OF A SET OF BASIC INDICATORS FOR AUTOMATEDASSESSMENT OF THE "HUMAN FACTOR" IN THE FIELD OF INFORMATION SECURITY

In this article, the author examines the reliability characteristics of the operating system operator, the types of his errors and related threats in the field of information security.
Keywords: automated assessment of the "human factor", analysis of the psychophysiological state, information security (IS), information security (IS), information and psychological security (IPS), information and psychological impact (IPI), automated systems operator (AS).

Современный этап развития защиты информации (ЗИ) характеризуется переходом к более широкому пониманию информационной безопасности (ИБ) в виде реализации комплексного подхода по двум основным направлениям: защиты информации и защиты от информации [1]. В свою очередь ЗИ становится одной из ключевых проблем современности. Выделяют три основных направления, подверженные информационным воздействиям: на технические системы и средства, общество и непосредственно на человека, т.н. «человеческий фактор» [6]. Это многоплановое понятие, под которым принято понимать принятия человеком ошибочных решений в конкретных ситуациях. Следует отметить, что возможности человека адекватно разобраться в сложившейся ситуации и принять верное решение могут снижаться, если он находится, образно говоря, в «плохом», неработоспособном состоянии. Существует множество причин появления такого состояния, а их появление может быть обусловлено влиянием факторов внешней среды, физиологии и психики конкретного человека и многими другими.

Кроме того, причинами могут быть утомление и неуверенность в своих силах, начинающееся заболевание, недостаточная подготовленность к данному виду деятельности и даже переживания как приятного, так и неприятного характера. Иногда психофизиологические, психологические характеристики и особенности человека не соответствуют уровням сложности поставленных и решаемых задач, вопросов или проблем. Характеристики, возникающие при взаимодействии человека и технических систем, связывают с человеческим фактором. Ошибки, связанные с проявлением данного фактора, как правило, непреднамеренные: человек выполняет ошибочные действия, оценивая их как правильные или наиболее подходящие в данном конкретном случае или ситуации.

Важным является предвидение возможности наступления такого состояния у человека в ходе повседневной работы, а также констатация его возникновения непосредственно в рабочий период. В течение этого времени у него периодически могут возникать неблагоприятные функциональные состояния, которые,

несомненно, будут сказываться на качестве принимаемых решений. В рабочих условиях существует ряд факторов, способствующих появлению усталости, воздействие которых на сотрудников создает предпосылки к аварийным ситуациям [2].

Однако в обеспечении ИБ сегодня нет возможности и методики автоматизированного и объективного учета и противодействия угрозам такого вида. В соответствии с этим обеспечение информационно-психологической безопасности (ИПБ) операторов автоматизированных систем (АС) является остроактуальным вопросом и определяет необходимость разработки теоретико-методологических основ обеспечения ИПБ целостности личности оператора АС. Вместе с тем и сама АС, и операторы АС в силу специфики своей профессиональной деятельности, подвержены внешним информационным воздействиям, последствия которых могут носить тяжелый деструктивный характер. Поэтому своевременное обнаружение факторов реализации информационных угроз для АС различного уровня может быть определено ассиметричными действиями по выявлению и пресечению специальных информационно-психологических воздействий (ИПВ). [5] Выявление индивидуально-личностных реакций операторов АС представляется возможным только при внедрении динамических методов анализа психофизиологического и функционального состояния непосредственно на рабочем месте.

На сегодняшний день основными средствами профессиональной психодиагностики являются анкеты, опросники и тесты различной степени сложности, в том числе и компьютерные. Но их применение требует длительного времени, большого числа методик и сопровождения со стороны профессионального контингента. Однако, при проведении экспресс-мониторинга состояния персонала в условиях стрессогенных факторов профессиональной деятельности, использование большого количества методик становится невозможным. Поэтому разработка моделей и методов экспресс-анализа и автоматизированной оценки психофизиологического состояния человека-оператора, а также методов регистрации реакции групп операторов на различные виды ИПВ в реальном времени является актуальной задачей с научной и практической точек зрения.

В качестве основы для проведения экспресс-анализа и автоматизированной оценки психофизиологического состояния персонала АС предлагается использовать следующие наборы типовых ошибок персонала связанных с их психофизиологическим состоянием, проявляющихся на базе аналогично типового набора надежностных (в психофизиологическом плане) характеристик оператора АС. Рассматриваемые типовые наборы представлены в таблице 1.

Таблица 1 – Типовые наборы для проведения экспресс-анализа и автоматизированной оценки психофизиологического состояния персонала АС [1, 3, 7]

Основные характеристики надежности оператора	**Виды ошибок**
1. Общая выносливость (сопротивляемость усталости к концу дня, особенно при монотонной работе). 2. Выносливость к экстренному напряжению и перенапряжению (необходимость выполнять максимальный объем работ за минимальные сроки). 3. Помехоустойчивость. 4. Спонтанная отвлекаемость (устойчивость к внутренним отвлекающим факторам). 5. Реакция на непредвиденные раздражители (в случае непредвиденных обстоятельств иногда наблюдается период «психической рефрактерности», когда восприятие концентрируется лишь на источнике этого раздражителя, не замечая другие обстоятельства).	1. Ошибки восприятия (не успел обнаружить, не сумел различить и др.). 2. Ошибки памяти (забыл, не успел запомнить, не сумел сохранить, воспроизвести и др.). 3. Ошибки мышления (не понял, не разобрался и др.). 4. Ошибки внимания

6. Переключаемость внимания (сокращение времени на переключение для выполнения новой задачи). 7. Устойчивость к действию факторов среды (температуре, давлению, вибрации, шуму, ускорению и т.п.)	(не сумел сосредоточиться, собраться, переключиться).

Общая (долговременная) выносливость. Количество ошибок и неточностей увеличивается к концу рабочего периода, особенно в случае большого объема работы, указывая на утомление центральной нервной системы. При монотонной, без переключений, работе эти сдвиги функционального состояния могут быть выражены еще резче. Отсюда следует, что надежность – это монотонно убывающая функция времени активной работы.

Выносливость к экстренному напряжению и перенапряжению. При дежурстве оператор сталкивается с аварийными ситуациями, когда требуется выполнение максимального объема работы за определенный (чаще всего минимальный) промежуток времени. Подвергается испытанию предельная пропускная способность оператора, способность быстро принимать решения. Факты наличия срывов, возникновения фазовых и невротических состояний в таких ситуациях указывают на практическую важность этой характеристики надежности.

Помехоустойчивость. Этим техническим термином можно по аналогии обозначить способность индивида противостоять отвлекающим внешним воздействиям, таким, как беспорядочные случайные шумы, посторонняя речь, движение посторонних предметов в поле зрения и т.д.

Спонтанная отвлекаемость. Снижение внимания вследствие внутреннего, спонтанного происхождения, особенно в условиях пассивного наблюдения, выполнения контролирующих функций и т.д.

Реакция на непредвиденные раздражители. Возникновение непредвиденной ситуации вызывает появление периода «психической рефрактерности», когда восприятие оператора и его интеллектуальные функции сужаются, концентрируясь на источнике неожиданного воздействия, а «деятельность» его по отношению к информации иного рода оказывается сниженной или вовсе заторможенной.

Переключаемость. Переход от выполнения одной задачи к другой требует времени. Величина этого «переходного интервала» при прочих равных условиях зависит от индивидуальных особенностей человека.

Устойчивость к действию факторов среды (температура, давление, влажность, шум, ускорение, гипоксия и т.д.). Этот вид функциональной устойчивости представляется весьма важным аспектом надежности. В отношении некоторых факторов устойчивость к их действию связана с силой нервной системы: повышение слуховых порогов при действии мощных шумов тем больше, чем ниже пороги данного индивида. Но более чувствительные индивиды обладают, как правило, более слабой нервной системой, следовательно, «слабые» испытуемые более подвержены утомляющему действию сверхсильной звуковой стимуляции.

Предложенный набор для проведения экспресс-анализа и автоматизированной оценки психофизиологического состояния персонала АС позволит сформировать необходимый базис для построения автоматизированной системы оценки уязвимости АС различного назначения от угроз информационной безопасности связанных с непреднамеренными вариантами реализации такого рода угроз. В качестве материальной основы фиксации данного набора могут выступать маркеры на основе анализа элементов клавиатурного почерка и датчиков психофизического состояния оператора АС

Перечень использованной литературы и источников:

1. Гатчин Ю.А., Сухостат В.В., Куракин А.С., Донецкая Ю.В. Теория информационной безопасности и методология защиты информации – 2-е изд., испр. и доп. – СПб: Университет ИТМО, 2018. – 100 с.

2. Каретников В.В. Исследование влияния усталости судоводителя на процесс обеспечения безопасности судоходства / В.В. Каретников, С.В. Козик, И.А. Соколова // Вестник Государственного университета морского и речного флота имени адмирала С.О. Макарова. – 2017. Т. 9. - № 2. – С. 272–279 (г. Санкт-Петербург).
3. Леонова А.Б. Функциональные состояния: человека в трудовой деятельности: Учебное пособие / А.Б. Леонова, В.И. Медведев. – Москва: Московский университет, 1981. – 112 с.
4. Мельников В.П. Информационная безопасность и защита информации: учебное пособие для студентов высших учебных заведений / В.П. Мельников, С.А. Клейменов. М. Петраков; под. ред. С.А. Клейменова. – Москва: ИЦ «Академия», 2009. – 336 с.
5. Петрик В.М., Остроухов В.В. Штоквиш О.А. и др. Современные технологии и средства манипулирования сознанием, ведения информационных войн и специальных информационных операций: Учебное пособие. – Москва: Росава, 2006. – 208с.
6. Руководство по обучению в области человеческого фактора: Утверждено Генеральным секретарем и опубликовано с его санкции ИКАО. 1-е издание [Электронный ресурс]. – Москва: Международная организация гражданской авиации (Федеральное агентство воздушного транспорта Министерства транспорта Российской Федерации), 1998. – 198с. – URL: http://www.sparcatc.ru/files/ICAO_Doc-9683-Rukovodstvo-po-obucheniyu-v-oblasti-chelovecheskogo-faktora-pdf.io.pdf.
7. Сухостат В.В. Модель и методы оценки информационной защищенности оператора автоматизированных систем: дис. …канд. тех. наук: 05.11.19 / В.В. Сухосват. – СПб.: СПб НИУ ИТМО, 2014. – 172с.

3.3. ПОДГОТОВКА КАДРОВ ДЛЯ IT-ОТРАСЛИ И КОНФЛИКТ ИНТЕРЕСОВ ЗАКАЗЧИКОВ И ИСПОЛНИТЕЛЕЙ

На сегодняшний день цифровая трансформация для Российской Федерации во всех сферах жизни страны (экономика, политика, обороноспособность и социалка) является главным стратегическим приоритетом. Необходимость перехода страны на новый технологический уровень отражена в ряде стратегических документов, и основой этого перехода является образование всех уровней и в различных образовательных учреждениях/организациях [1, 4–8]. Но, реалии дня показывают, что в реализации требования дня, кроме социально-экономических проблем для образовательных учреждений/организаций стал вопрос конфликта интересов между IT-отраслью (заказчик) и исполнителем (вуз, ссуз, учебный цент). Устранить проблемы в образовательном процессе, и конфликта интересов может только благодаря интеграции вуза и IT-компаний.
Ключевые слова: IT-компания, вуз/ссуз, информатизация общества, информация, конфликт интересов исполнителей и заказчика в подготовке специалистов, подготовка кадров IT-отрасли, преподаватель, профессиональная деятельность, студент, ФСТЭК ДФО, цифровая трансформация.

TRAINING OF PERSONNEL FOR THE IT INDUSTRY AND THE CONFLICT OF INTERESTS OF CUSTOMERS AND PERFORMERS

Today, digital transformation for the Russian Federation in all spheres of the country's life (economy, politics, defense capability and social sphere) is the main strategic priority. The need for the country's transition to a new technological level is reflected in a number of strategic documents, and the basis of this transition is education at all levels and in various educational institutions/organizations [1, 4-8]. But, the realities of the day show that in implementing the requirements of the day, in addition to socio-economic problems for educational institutions/organizations, there was a conflict of interest between the IT-industry (customer) and the contractor (university, secondary school, educational center). Problems in the educational process and conflicts of interest can be eliminated only through the integration of the university and IT companies.
Keywords: IT company, university/college, informatization of society, information, conflict of interests between performers and the customer in training specialists, training of IT industry personnel, teacher, professional training.

... подготовка кадров для ИТ-отрасли, зависит не только от увеличения финансирования данного направления, но прежде всего от совместной деятельности образовательных

учреждений и предприятий ИТ-отрасли.

Чернышенко Д.М.
Заместитель Председателя
Правительства Российской Федерации

Подготовка кадров для предприятий/организаций IT-отрасли на текущий момент времени является актуальной и сложной для быстрого решения задачей. Сложной не в силу слабой научной проработки предмета нашего рассмотрения или отсутствие необходимых объективных условий, а в силу множества негативных факторов, влияющих на данный вид подготовки кадров. Именно негативные факторы создают тот фон «…конфликтности, неопределенности и противоречий…» [9] между всеми вовлеченными в этот процесс субъектами: «исполнителями в лице вузов и заказчиками в лице государственных и коммерческих компаний-потребителей кадров IT-сферы» [13].

Состоявшийся в ноябре 2023 года Координационное совещание по вопросу подготовки специалистов по информационной безопасности в Управлении ФСТЭК ДФО, IT-компаний с представителями вузов и ссузов ДФО, ведущих подготовку работников по направлению «Информационная безопасность» (ИБ) еще отчётливее обозначило конфликт интересов и разницу во взглядах на процесс подготовки кадров в целом и специалистов ИБ в частности.

Так, руководством ФСТЭК ДФО было указано на недостатки в обучении кадров, слабую практическую подготовку выпускников, неспособность молодых «специалистов» решать актуальные задачи с учетом текущей социальной, правовой, международной обстановки, в условиях открытого противодействия стран «коллективного Запада», многочисленных санкций и вооруженного противостояния того же «коллективного Запада и России на полях СВО.

Представители образовательных заведений также показали свою озабоченность, по существу, заявленных регулятором (ФСТЭК) претензий, но в свою очередь указали на факторы усложняющие, а в ряде случаев и препятствующие подготовке кадров способных стопроцентно удовлетворять заявленным требованиям заказчика.

К наиболее существенным факторам были отнесены недостатки финансирования, недостатки в подготовке штатов, а также слабая учебно-материальная база учебного процесса и многие другие.

В итоге, взаимные претензии прямо указали на конфликт интересов и разные взгляды на происходящие процессы, противоречия в подходах и методиках решения обозначенной задачи. Даже поверхностный анализ перечисленных факторов свидетельствует о системном конфликте исполнителя в лице учебных заведений и заказчиков - компаний, предприятий, организаций как госсектора, так и бизнеса.

Логично возникает вопрос, а возможно ли преодоление этого кризиса отношений? Увы, но с сожалением можно констатировать тот факт, что преодолеть сложившуюся ситуацию в полной мере не представляется возможным. Вместе с тем, понизить конфликтность, путем устранения или снижения степени негативного влияния указанных факторов, можно и нужно, но в такую работу необходимо включать и других акторов рассматриваемых отношений.

Так, техническая оснащенность учебного процесса напрямую связана с финансовыми возможностями учебного заведения, но оные не зависят от вуза, а входят в компетенцию учредителя. Более того, разработчики и производители IT-продукции имеют главной целью получение прибыли (сверхприбыли), а не обеспечение потребителей (вузов) своей продукцией. Как следствие, ситуация еще больше усугубилась в условиях санкций и СВО, а разработчики и производители, будучи «третьей стороной» рассматриваемого процесса, вовсю используют административный ресурс и стремятся получить сверхвыгоду из своего монополизма. Встречаются даже факты открытого шантажа, мол «... вы обязаны отказаться от использования

зарубежной продукции и приобрести ***нашу*** продукцию по заявленным ценам, как с единственным поставщиком...». Полагаем, что такие ситуации необходимо рассматривать с позиции «картельного» сговора или принуждения к сделкам в обход действия 2-х законов России: «О контрактной системе в сфере закупок товаров, работ, услуг для обеспечения государственных и муниципальных нужд» от 05.04.2013 № 44-ФЗ [2] и «О закупках товаров, работ, услуг отдельными видами юридических лиц» от 18.07.2011 № 223-ФЗ [3].

Помимо этого, российский IT-бизнес явно не заинтересован в «долгих» взаимоотношениях и без внешнего воздействия не будет вкладываться в «долгий процесс» - подготовки кадров, т.к. – «прибыль ему нужна здесь и сейчас, а льготы и преференции от государства в лице Минцифры России не будут вечными и безграничными» [14]. Помимо этого, IT-компании регионального масштаба и филиальная сеть крупных операторов связи и банковского сектора проводят исключительно потребительскую политику. Поскольку государством ежегодно увеличиваются КЦП на инженерные специальности и количество выпускников растет, то новые работники в указанные организации в любом случае придут, т.к. нужно же где-то дипломированным специалистам работать! Вкладывать средства в техническое оснащение указанные выше субъекты экономических отношений абсолютно не заинтересованы, а в случае прямого к ним обращения всегда ссылаются на тот факт, что субъекты принятия решения находятся либо в западной части России, либо прямо указали на запрет такой деятельности. Считаем, что все расходы по увеличению набора в вузы, установлению контрольных цифр приема должны взыскиваться именно с потребителей, т.е. IT-отрасли. Льготы по налогообложению могут быть предоставлены исходя из объемов вложенных средств в образование и социальную сферу - так как это делается в странах с более развитой экономикой.

Полагаем, что решение задачи по техническому и программному оснащению вузов возможна любо проверенным, но не работающим методом рыночных отношений, либо административно-распорядительным «госзаказом». Упование на рыночный регулятор уже привел IT-сферу к сложившейся ситуации, когда «играющие в долгую» зарубежные компании не позволили сформировать конкурентный российский IT-продукт, а образовательные стандарты были на уровне Минобрнауки России ориентированы на применение в обучении американского ПО и зарубежной техники. Ярчайшим примером тому является проверка навыков работы российских конкурсантов среднего профессионального обучения в WSR на оборудовании «поэтому». Формирование же «Госзаказа», если это только не связано с производством продукции ВПК (сейчас принято говорить ОПК) для нужд СВО, отторгается на всех уровнях принятия решений. Возможный выход из сложившейся ситуации в выработке «среднего» варианта - целевого финансирования в производство необходимого продукта и плановое оснащение вузов по примеру снабжения воинских частей продукцией ВПК (ОПК), либо целевое финансирование закупочных процедур учебными заведениями. Последний вариант более предпочтителен, хотя, так же несет в себе ряд угроз: резкий рост стоимости продукции, выносимой на торги, возможность «ценового сговора», сговора «трёх коммерческих предложений», отказ участвовать в объявляемых конкурсах и т.п.

Еще одна проблема, озвученная в ходе указанного координационного совещания, касалась дефицита профессорско-преподавательского состава (ППС) и педагогических работников (ПР). Данная проблема не новая в силу катастрофического роста показателя «среднего возраста», но факторы, ее определяющие так же, не входят в сферу работы учебных заведений. К таковым можно отнести не только привычные и уже раздражающие факторы низкой зарплаты и низкого авторитета ученых, но и дефицит инженерных кадров, мизерное количество кандидатов и докторов технических наук по ИТ-специальностям, отток не малого количества специалистов из России

(«релокация и удаленка»), инфантильное и безответственное отношение молодых педагогов к работе усугубившееся в условиях «удаленной» работы в период ковидных ограничений [11, 12, 13].

Это так же не полный перечень негативных факторов, обострившихкадровую проблему вузов, но каждый из них требует принятия комплексных мер, которые в большей мере не входят в компетенцию администрации учебных заведений.

К примеру, привлечение практических работников IT-компаний к учебному процессу вызывает обоснованные затруднения, так. ставка такого сотрудника настолько мала, что может составлять за месяц работы менее 10 тыс. рублей. Устанавливать же персональную повышенную ставку возможно только при наличии внебюджетных доходов, что в условиях дотационности бюджетов вузов крайне затруднительно. При этом не нужно забывать, что не каждый специалист-практик готов к педагогической работе, т.к. сделать работу порой гораздо легче, чем обучить этому других.

Безусловно, помимо обозначенных выше негативных факторов, носящих внешний или многосубъектный характер есть и исключительно внутривузовские. Наиболее распространенными, по нашему мнению, являются традиционность преподавания, многолетняя «привычка» чтения лекций, написанных годы тому назад, описательность материала и акцентированность на собственных научных работах. Противодействие указанным факторам возможна в рамках работы Учебно-методических советов (УМС), но с учетом дефицита кадров, предпенсионного возраста большинства работников и «диктатуры» работников по отношению к работодателям, это так же вызывает определенные затруднения.

Таким образом, подводя итог всему вышеуказанному следует сделать несколько вывод, что подготовка квалифицированных кадров может быть достигнута лишь в реализации мер комплексного характера с активным участием и образовательное учреждение (вузов/ссуз/учебный цент), и учредителей, и регуляторов, и потребителей (заказчиков). Вуз/ссуз/учебный цент со своей стороны оперативно вносят коррективы в образовательные программы, обеспечивая тем самым условия для конкурентоспособности выпускников. При этом у IT-компаний появляется возможность ставить задачу по осуществлению подготовки специалистов «по заказу» [9], принимать «непосредственное участие в реализации совместных проектов, выступать партнерами научных мероприятий, разрабатывать учебно-методические материалы, предоставлять базы для практики и стажировки – т.е. «… быть полноправным участником учебно-воспитательного процесса» [10] в образовательном учреждении.

Перечень использованной литературы и источников:

1. Российская Федерация. Закон о образовании в Российской Федерации: федер. закон от 29.12.2012 №273-ФЗ (в ред. от 25.12.2023 № 685-ФЗ) // СПС «GARANT.ru»

2. Российская Федерация. Законы. О контрактной системе в сфере закупок товаров, работ, услуг для обеспечения государственных и муниципальных нужд: федер. закон от 05.04.2013 44-ФЗв ред. от 25.12.2023 № 625-ФЗ) // СПС «GARANT.ru».

3. Российская Федерация. Законы. О закупках товаров, работ, услуг отдельными видами юридических лиц: федер. закон от 18.07.2011 № 223-ФЗ // СПС «GARANT.ru»

4. Российская Федерация. Президент. О Стратегии научно-технологического развития Российской Федерации: Указ президента Российской Федерации от 01.12.2016 г. № 642. (в ред. от 15.03.2021 // СПС «GARANT.ru»

5. Российская Федерация. Президент. Об утверждении приоритетных направлений развития науки, технологий и техники в Российской Федерации и перечня критических технологий Российской Федерации: Указ Президента РФ от 07.07.2011 № 899 (в ред. Указа Президента РФ от 16.12.2015 № 623 // СПС «GARANT.ru».

4. Российская Федерация. Президент. Стратегия развития информационного общества на 2017–2030 гг.: Указ Президента РФ от 09.05.2017 № 203 // СПС «GARANT.ru».

5. Российская Федерация. Правительство Российской Федерации. Национальная программа «Цифровая экономика Российской Федерации» (Федеральный проект «Кадры для цифровой экономики»):

Постановление Правительства Российской Федерации от 02.03.2019. №234 // Российская Федерация. Правительство Российской Федерации. О утверждении Государственной программы Российской Федерации «Развитие образования»: Постановление Правительства РФ от 26 декабря 2017 г. №1642 // СПС «KREMLIN.ru».
6. Российская Федерация. Правительство Российской Федерации. О создании Российского фонда развития информационных технологий»: Постановление Правительства РФ от 24.01.2017 № 57 (с изм. и доп. от 17. 06.2021 г.) // СПС «KREMLIN.ru».
7. Российская Федерация. Правительство Российской Федерации. О утверждении Государственной программы Российской Федерации «Развитие образования»: Постановление Правительства РФ от 26.12.2017 № 1642-р // СПС «KREMLIN.ru».
8. Российская Федерация. Правительство Российской Федерации. Об утверждении Программы фундаментальных научных исследований в Российской Федерации на долгосрочный период (2022–2030гг.): Распоряжение правительства РФ от 31.12.2020 № 3684-р // СПС «DIGITAL.gov.ru».
9. Буньковский Д.В. Европейский опыт взаимодействия малого, среднего и крупного производственного предпринимательства / Д.В. Буньковский // Известия БГУЭП. – 2011. – № 3. – С. 27
10. Вадова Л.Ю. Система взаимодействия вуза и работодателей в подготовке будущих специалистов / Л.Ю. Вадова // Международный журнал прикладных и фундаментальных исследований. – 2016. – № 5-2. – С. 311–315.
11. Климова Ю.О., Усков В. С.К вопросу подготовки кадров для ИТ-отрасли в условиях цифровизации // Вестник КемГУ. Серия: Политические, социологические и экономические науки. – 2020. - № 2(16). – С. 222–231.
12. Кулагина Н.А. Подготовка кадров для цифровой экономики: Тренды и проблемы / Н.А. Кулагина, А.Н. Лысенко, С.П. Новиков // Вестник ПНИПУ. Социально-экономические науки. – 2022. - № 3. – С. 148-160.
13. Селицкая С.В. Интересы взаимодействия вуза и IT-компаний / С.В. Селицкая // 12-я Международная научно-методическая конференция: «Высшая школа: проблемы и перспективы» (Минск, 22–23 октября 2015 г.) В 2 ч. Ч. 1. – Минск: БГУ, 2015. – С. 136-139.
14. Трофимова И.Н. Российская образовательная политика и конфликты интересов в сфере инноваций / И.Н. Трофимова // Полис. Политические исследования. – 2021. - № 5. – С. 25-38.

3.4. ГОСУДАРСТВЕННАЯ СИСТЕМА АТТЕСТАЦИИ И ЛИЦЕНЗИРОВАНИЯ В СФЕРЕ ИНФОРМАЦИОННОЙ БЕЗОПАСНОСТИ

В статье рассмотрены некоторые проблемные вопросы системы аттестации объектов информатизации в Российской Федерации.
Ключевые слова: государственная система аттестации объектов информатизации, информационная безопасность (ИБ), объекты информатизации.

STATE SYSTEM OF CERTIFICATION AND LICENSING IN THE FIELD OF INFORMATION SECURITY

The article discusses some problematic issues of the certification system for informatization objects in the Russian Federation.
Keywords: state system of certification of informatization objects, information security, informatization objects.

Аттестация и лицензирование позволяют проверить и подтвердить действительную степень защищенности информационных систем, успешность внедрения средств информационной безопасности, а также степень защищенности информации в соответствии с требованиями нормативно-правовых актов Российской Федерации.

ФСТЭК Росси:
Положение об аккредитации органов
по аттестации объектов информатизации по
требованиям безопасности информации.

В статье 1 закона Российской Федерации «О безопасности» - безопасность

определена как: «состояние защищенности жизненно важных интересов личности, общества и государства от внутренних и внешних угроз» [1].

Жизненно важные интересы – это совокупность потребностей, удовлетворение которых надежно обеспечивает существование и возможности прогрессивного развития личности, общества и государства [1].

В «Доктрине информационной безопасности Российской Федерации» и «О Стратегии национальной безопасности Российской Федерации даны следующее определение: «Информационная безопасность Российской Федерации – это состояние защищенности ее национальных интересов в информационной сфере, определяющихся совокупностью сбалансированных интересов личности, общества и государства» [2,3].

Исходя из этих нормативных посылов при проведении работ со сведениями соответствующей степени конфиденциальности (секретности) системы информатизации должны (могут) быть аттестованы на соответствие требованиям по безопасности информации.

Государственная система аттестации объектов информатизации устанавливает основные принципы, организационную структуру, порядок проведения аттестации, а также порядок контроля и надзора за эксплуатацией аттестованных объектов информатизации.

Под ***объектами*** информатизации, аттестуемыми по требованиям безопасности информации, понимаются автоматизированные системы различного уровня и назначения, системы связи, отображения и размножения вместе с помещениями, в которых они установлены, предназначенные для обработки и передачи информации, подлежащей защите, а также сами помещения, предназначенные для ведения конфиденциальных переговоров.

Система аттестации объектов информатизации по требованиям безопасности информации является составной частью единой государственной системы сертификации средств защиты информации и аттестации объектов информатизации по требованиям безопасности информации. Деятельность системы аттестации организуют уполномоченные федеральные органы по сертификации продукции и аттестации объектов информатизации по требованиям безопасности информации.

Под ***аттестацией*** объектов информатизации понимается комплекс организационно-технических мероприятий, в результате которых посредством специального документа – ***«Аттестата соответствия»*** подтверждается, что объект соответствует требованиям стандартов или иных нормативно-технических документов по безопасности информации, утверждённых уполномоченными федеральными органами исполнительной власти. Наличие на объекте информатизации действующего «Аттестата соответствия» даёт право обработки информации с определённым уровнем конфиденциальности и в указанный в «Аттестате соответствия» период времени.

При аттестации объекта информатизации подтверждается его соответствие требованиям по защите информации от несанкционированного доступа, в том числе от компьютерных вирусов, от утечки за счёт побочных электромагнитных излучений и наводок при специальных воздействиях на объект (высокочастотное навязывание и облучение, электромагнитное и радиационное воздействие), от утечки или воздействия на неё за счёт специальных устройств, встроенных в объекты информатизации.

Аттестация проводится уполномоченными органами по аттестации объектов информатизации, аккредитованными федеральными органами исполнительной власти Правила аккредитации определяются действующими в соответствующих системах сертификации положениями. В системе сертификации ФСТЭК России разработано и утверждено 25 ноября 1994 г. «Положением об аккредитации органов по аттестации объектов информатизации по требованиям безопасности информации» [12]. Каждый такой орган имеет лицензию на право выполнения работ в области защиты информации и «Аттестат аккредитации». Виды работ, которые он может выполнять, указываются в

области аккредитации, являющейся приложением к «Аттестату аккредитации». В своей деятельности органы по аттестации руководствуются нормативно-методическими документами ФСТЭК России.

Аттестат соответствия утверждается руководителем органа по аттестации объектов информатизации, который и несёт юридическую и финансовую ответственность за качество проведённых работ. Кроме того, органы по аттестации несут ответственность за обеспечение сохранности государственных и коммерческих секретов, а также за соблюдение авторских прав разработчиков аттестуемых объектов информатизации и их компонент.

Аттестация информационных систем может производиться в соответствии с Руководящим документом ФСТЭК России «Автоматизированные системы. Защита от несанкционированного доступа к информации. Классификация автоматизированных систем и требования по защите информации» [13].

Основные признаки группировки в различные классы связаны с:

- наличием в АС информации различного уровня конфиденциальности;
- уровнем полномочий субъектов доступа АС на доступ к конфиденциальной информации (одинаковый или разный);
- режимом обработки данных в АС (коллективный или индивидуальный).

Для каждого класса сформулирован определённый набор требований для подсистем:

- управления доступом;
- регистрации и учета;
- криптографической;
- обеспечения целостности.

Группа 1 классифицирует многопользовательские АС, в которых одновременно обрабатывается и (или) хранится информация разных уровней конфиденциальности, и не все пользователи имеют право доступа ко всей информации АС. Группа содержит пять классов: **1Д, 1Г, 1В, 1Б и 1А.**

Группа 2 классифицирует АС, в которых пользователи имеют одинаковые права доступа (полномочия) ко всей информации АС, обрабатываемой и (или) хранимой на носителях различного уровня конфиденциальности. Группа содержит два класса: **2Б** и **2А.**

Группа 3 классифицирует АС, в которых работает один пользователь, допущенный ко всей информации АС, размещённой на носителях одного уровня конфиденциальности. Группа содержит два класса: **3Б** и **3А.**

Защита информации является общегосударственной проблемой, т.к. это напрямую связано с обеспечением его суверенитета. Такое регулирование опирается на государственную систему безопасности и на свод законов по лицензированию деятельности в сфере защиты информации.

Лицензия – выдаваемое уполномоченным лицом (лицензиаром) юридическим и физическим лицам (лицензиатам) разрешение на совершение определенных действий, без которого совершение таких действий признается неправомерным [8].

Лицензирование – это процесс, осуществляемый в отношении таких категорий, как «деятельность» (виды деятельности) и «субъект» (физическое лицо, предприятие, организация или иное юридическое лицо), когда некоторый субъект в результате проведения комплекса мероприятий, состав, правила и порядок осуществления которых предписываются законодательными и нормативными актами, получает право на осуществление определенного вида деятельности. Это право закрепляется и оформляется в виде официальных документов, виды и статус которых также предписываются нормативными актами. За органом, уполномоченным на проведение лицензионной деятельности, закрепляется право на осуществление контроля за деятельностью лицензиата. Важно подчеркнуть, что активную роль в процессе

лицензирования играют обе стороны: орган, наделяющий кого-либо правом деятельности, и субъект, получающий указанное право. Получить право на осуществление деятельности, подлежащей лицензированию, может не каждый, а лишь субъект, отвечающий определенным критериям, которые заранее определяются правилами проведения лицензирования и требованиями к предприятию-заявителю. Таким образом, субъектом лицензирования становится лишь то физическое или юридическое лицо, которое представляет все необходимые и правильно оформленные документы и удовлетворяет соответствующим критериям [7, 8, 9].

Сертификация – это подтверждение соответствия продукции или услуг установленным требованиям или стандартам.

Сертификат на средство защиты информации – документ, подтверждающий соответствие средства ЗИ требованиям по безопасности информации.

Законодательной и нормативной базой лицензирования и сертификации в области защиты информации в Российской Федерации являются Законы, Постановления Правительства, Указы Президента и иные подзаконные акты.

Полный перечень видов деятельности в области защиты информации, подлежащих обязательному государственному лицензированию, определён в Законе РФ «О государственной тайне» [2] и Федеральном законе «О лицензировании отдельных видов деятельности» [8]. В законе РФ «О государственной тайне» определены лицензируемые виды деятельности в области защиты информации, содержащей сведения, отнесённые к государственной тайне, а в Законе РФ «О лицензировании отдельных видов деятельности» – в области защиты конфиденциальной информации [2].

В ст. 27 Закона РФ «О государственной тайне» указано, что: «допуск предприятий, учреждений и организаций к проведению работ, связанных с использованием сведений, составляющих государственную тайну, созданием средств защиты информации, а также с осуществлением мероприятий и (или) оказанием услуг по защите государственной тайны, осуществляется путём получения ими лицензий в порядке, устанавливаемом Правительством Российской Федерации. Во исполнение данной статьи закона Правительством РФ было принято Постановление Правительства «О лицензировании деятельности предприятий, учреждений и организаций по проведению работ, связанных с использованием сведений, составляющих государственную тайну, созданием средств защиты информации, а также с осуществлением мероприятий и (или) оказанием услуг по защите государственной тайны», которым было утверждено одноимённое «Положение» [2].

Согласно этому «Положению», лицензия на проведение работ связанных с государственной тайной, выдается на основании результатов специальной экспертизы предприятия, учреждения и организации и государственной аттестации их руководителей, ответственных за защиту сведений, составляющих государственную тайну, расходы по проведению которых относятся на счет предприятия, учреждения, организации, получающих лицензию. Лицензия выдается претенденту при соблюдении им следующих условий [8]:

- выполнения требований нормативных документов по обеспечению защиты сведений, составляющих государственную тайну, в процессе выполнения работ, связанных с использованием указанных сведений;

- наличия в их структуре подразделений по защите государственной тайны и специально подготовленных сотрудников для работы по защите информации, количество и уровень квалификации которых достаточны для обеспечения защиты государственной тайны;

- наличия у них сертифицированных средств защиты информации.

Средства защиты информации должны иметь сертификат, удостоверяющий их соответствие требованиям по защите сведений соответствующей степени секретности.

Сертификация осуществляется на основании требований государственных стандартов и иных нормативных документов.

В заключение необходимо отметить, что лицензирование, аттестация и сертификация – это комплекс мероприятий главная цель которых обеспечение защиты гостайны – исключение утечки информации и, таким образом, исключение возможности нанесения организации ущерба, к которому эта утечка может привести.

Перечень использованной литературы и источников:

1. Российская Федерация. Законы. О безопасности: федер. закон от 28.12.2010 № 390-ФЗ (в последней редакции 10.07.2023 № 286-ФЗ) // СПС «КонсультантПлюс».
2. Российская Федерация. Законы. О государственной тайне: закон от 21.07.1993 № 5485-1 (в последней редакции от 04.08.2023 N 432-ФЗ) СПС «КонсультантПлюс».
3. Российская Федерация. Законы. О сертификации продукции и услуг: закон № 5485-1 от 10.06.93 (в последней редакции от 10.01.2003 № 15-ФЗ, с изм., внесенными Постановлением Конституционного Суда РФ от 22.11.2001 № 15-П) // СПС «КонсультантПлюс».
4. Российская Федерация. Законы. О защите прав потребителей: федер. закон от 09.01.1996 № 2-ФЗ (в последней редакции от 05.12.2022 № 478-ФЗ) // СПС «КонсультантПлюс».
5. Российская Федерация. Законы. Об информации, информатизации и защите информации: федер. закон от 27.07.2006 N 149-ФЗ (в последней редакции от 12.12.2023 №588-ФЗ) // СПС «КонсультантПлюс».
6. Российская Федерация. Законы. О стандартизации в Российской Федерации: федер. закон от 29.06.2015 № 162-Ф (в последней редакции от 30.12.2020 N 523-ФЗ) // СПС « KREMLIN.ru».
7. Российская Федерация. Правительство Российской Федерации. Об организации лицензировании отдельных видов деятельности: Постановления Правительства РФ от 21.11.2011 № 957 (с изм. и доп., вступ. в силу с 01.03.2022) // СПС «KREMLIN.ru».
8. Российская Федерация. Правительство Российской Федерации. О лицензировании деятельности предприятий, учреждений и организаций по проведению работ, связанных с использованием сведений, составляющих государственную тайну, созданием средств защиты информации, а также с осуществлением мероприятий и (или) оказанием услуг по защите государственной тайны: Постановление Правительства РФ от 15.04.1995 № 333 (в последней редакции от 03.02.2023 № 159) // СПС «PRAVO.gov.ru».
9. Российская Федерация. Правительство Российской Федерации. О сертификации средств защиты информации: Постановление Правительства РФ от 26.06.1995 № 608 (в последней редакции от 21.04.2010 № 266) // СПС «PRAVO.gov.ru».
10. 2. Российская Федерация. Президент Российской Федерации. Доктрина информационной безопасности Российской Федерации: Указ Президента Российской Федерации от 05.12.2016 № 646 //» KREMLIN.ru».
11. Российская Федерация. Президент Российской Федерации. О Стратегии национальной безопасности Российской Федерации: Указ Президента РФ от 02.07.2021 № 400 // СПС «KREMLIN.ru».
12. Российская Федерация. ФСТЭК России. Положение об аккредитации органов по аттестации объектов информатизации по требованиям безопасности информации. Утверждена решением Государственной технической комиссии при Президенте Российской Федерации от 25 ноября 1994 г. [Электронный ресурс]. – URL: http://legion-inform.ru/zakonodatelstvo/polozhenie-po-attestacii-obektov-in.
13. Российская Федерация. ФСТЭК России. Автоматизированные системы. Защита от несанкционированного доступа к информации. Классификация автоматизированных систем и требования по защите информации: Утверждена решением Государственной технической комиссии при Президенте Российской Федерации от 30 марта 1992г. [Электронный ресурс] // Сборник руководящих документов по защите информации от несанкционированного доступа. – С. 11-16. – URL: https://www.msu.ru/info/is/docs/6/rd.pdf.

3.5. РЕАЛИЗАЦИЯ ТЕХНОЛОГИЙ ФОРМИРОВАНИЯ СУБЪЕКТНОЙ ПОЗИЦИИ СТУДЕНТОВ В КОНТЕКСТЕ ОБЕСПЕЧЕНИЯ БЕЗОПАСНОСТИ ИНФОРМАЦИИ

В данной статье описаны механизмы формирования и становления студентов как субъектов духовно-нравственной культуры при изучении учебных дисциплин. Рассмотрена возможность реализации полученного опыта в своей последующей профессиональной деятельности для обеспечения правил информационной безопасности (ИБ).

Ключевые слова: адекватный эмоциональный отклик, защита информации, информационная безопасность (ИБ), рефлексия, субъектная позиция, технология, уровни усвоения.

IMPLEMENTATION OF TECHNOLOGIES FOR FORMING THE SUBJECTIVE POSITION OF STUDENTS IN THE CONTEXT OF ENSURING INFORMATION SECURITY

This article describes the mechanisms of the formation and development of students as subjects of spiritual and moral culture when studying academic disciplines. The possibility of implementing the experience gained in one's subsequent professional activities to ensure information security rules is considered.

Key words: adequate emotional response, information protection, information security (IS), reflection, subject position, technology, levels of assimilation.

Информационная безопасность (ИБ) – это состояние защищенности общества и государства, отдельного гражданина от информационно-технического воздействия на информационную инфраструктуру [1]. То есть это состояние защищенности общества от недобросовестной информации либо от ее разглашения. Базовые нормы обеспечения ИБ закреплены в Федеральном законе «Об информации, информационных технологиях и о защите информации» [2].

Общеизвестно, что для обеспечения защиты информации наряду с информационными, техническими и физическими средствами, не следует исключать влияние на безопасность непреднамеренных ошибок пользователя (человеческий фактор). Обычно они возникают случайно из-за невнимательности, небрежности, непонимания и т.д. или воздействия третьей стороны. Наряду с использованием технических уязвимостей ИТ-технологий возможно проникновение посредством инструментов социальной инженерии - манипуляция сознанием человека для того, чтобы заставить пользователя раскрыть информацию или предоставить доступ к сетям данных.

Учитывая сложное взаимодействие в процессе информационной защиты безопасности человеческого, материального факторов и окружающей среды, полное устранение угроз безопасности невозможно. Влияние некоторых из этих факторов можно минимизировать.

Опишем реализацию технологий формирования и становления студентов как субъектов саморазвития при изучении учебных дисциплин, которые позволят минимизировать риски и угрозы ИБ со стороны пользователя.

Прежде всего, студентам на занятиях необходимо осмыслить целевое взаимодействие систем учения и преподавания, воспитания и самовоспитания как средство становления их субъектной позиции, то есть усвоить предметную область целей и технологий их достижения.

Представим механизмы, обеспечивающие формирование субъектной позиции студентов в аспекте самовоспитания духовно-нравственной культуры [3, с.68-74].

На первоначальном этапе развития позиции нужно научиться моделировать свое поведение и отношения в любой ситуации, то есть проявлять себя как субъект, обладающий духовно-нравственной культурой, так как духовность проявляется в деятельности, которую моделирует субъект.

Работа над мировоззренческой целью опосредованно связана с информацией по теме занятия. Человек как субъект должен относиться к любой деятельности, если она направлено на его созидание, положительно. Причем, положительное отношение – это творческая духовно-познавательная деятельность по осмыслению своего поведения, что получило название рефлексии.

Преподаватель на каждом занятии обеспечивает усвоение студентами трех аспектов мировоззренческой цели и моделирует взаимодействие для анализа понимания ими технологии достижения. Информационный аспект обеспечивается на 1-м и 2-м уровнях усвоения (УУ), составляющих «дерево цели» репродуктивным методом для организации деятельности на занятии. Мотивационный аспект требует адекватного эмоционального отклика на цели, например, удовлетворение, гордость за

полученный результат. Операционный аспект цели состоит в принятии мировоззренческой цели для моделирования поведения, предполагающего сотрудничество при управлении взаимодействием систем для решения, спрогнозированных нами целей.

Рассмотрим технологию, названную алгоритмом управленческого решения, и овладение ею студентами на 1-м и 2-м УУ на примере решения задачи или любого задания. Обычно под задачей понимают объект мыслительной деятельности, содержащий требование некоторого практического преобразования или ответа на теоретический вопрос посредством поиска условий, выявляющих отношение между известными и неизвестными элементами проблемной ситуации. После выполнения всех операций и получения ответа на поставленный вопрос задачи, необходимо осуществить рефлексию (самоанализ) полученного результата:

- соотнести полученный результат с вопросом;
- продумать эффективность выполненных операций;
- оценить необходимость сохранения способа, использованного для выполнения задания в дальнейшем при выполнении подобных заданий;
- осуществить рефлексию достижения мировоззренческой цели и адекватность эмоционального отклика, который сопровождал субъекта познания при выполнении задания;
- проанализировать, происходит ли формирование профессионально-управленческих способностей, то есть становления субъектной позиции.

Отметим, что решение задачи для студентов не самоцель, а способ приобретения опыта логики моделирования деятельности, отношений к ней и управления ее осуществлением. Роль управления выполняет операционный алгоритм, являющийся средством становления студентов субъектами своего саморазвития: интеллектуального, духовно-нравственного и профессионального потенциалов.

Если ситуация для студента окажется нестандартной, что в жизни довольно часто встречается, то он оказывается в точке бифуркации, требующей самостоятельного выбора. Ситуация ставит студента перед фактом творчески-созидательного подхода (3-й УУ с адекватным отношением).

Итак, целевая организация взаимодействия преподавателя и студентов на занятиях, куда аксиоматически встраивается предметная область знаний, предполагает для студентов:

- осмысление целей;
- разработку адекватных целям технологий;
- моделирование систем познания и поведения и их реализацию;
- осуществление рефлексии по степени достижения целей.

Рефлексия имманентно, позволяет фиксировать динамику становления субъектной позиции студентов, динамику приобретения опыта самоуправления. Такой опыт, приобретаемый в системе обучения, будущие специалисты смогут экстраполировать в профессиональную деятельность для решения проблем, используя интеллектуальный потенциал, нравственную позицию.

Одной из задач второго этапа является организация рефлексивной деятельности по определению механизмов достижения поставленных целей. Такие ситуации предполагают мыслительную деятельность, состоящую не в перечислении последовательности и количестве выполненных работ, а в фиксировании сущностной характеристики познавательной деятельности по моделированию интеллектуальной и духовно-нравственной систем на конкретном занятии. Деятельность педагога при этом осуществляется с использованием объяснительно-иллюстративного метода. Это принципиально важно, так как опыта по рефлексивной деятельности у студентов нет. Для осуществления рефлексивной деятельности преподавателя по достижению

содержательно-образовательных целей при изучении учебного материала разработаны алгоритмы, представленные рисунками 1 и 2.

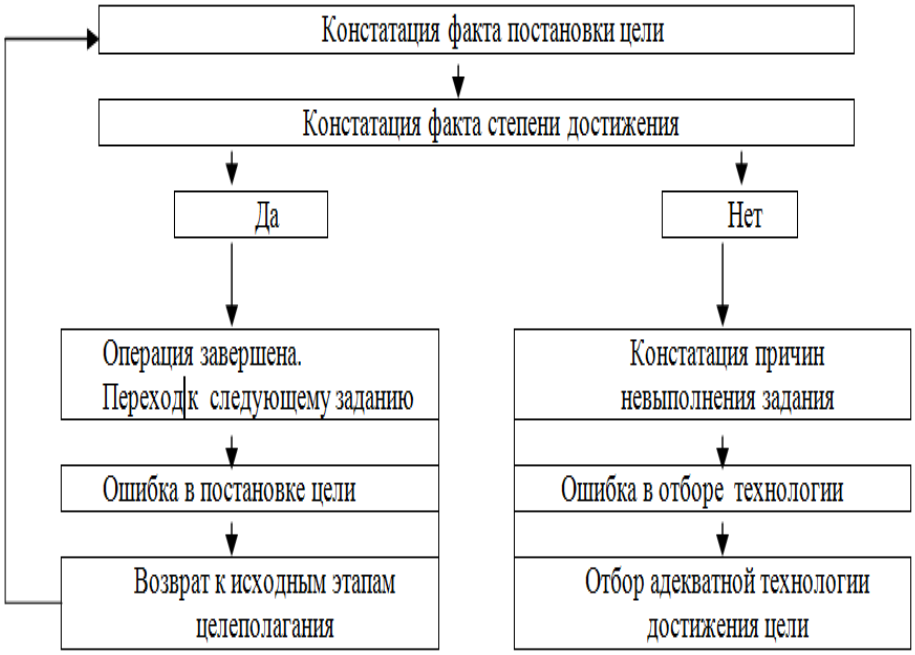


Рисунок 1– Алгоритм рефлексии содержательно-образовательной цели (1УУ)

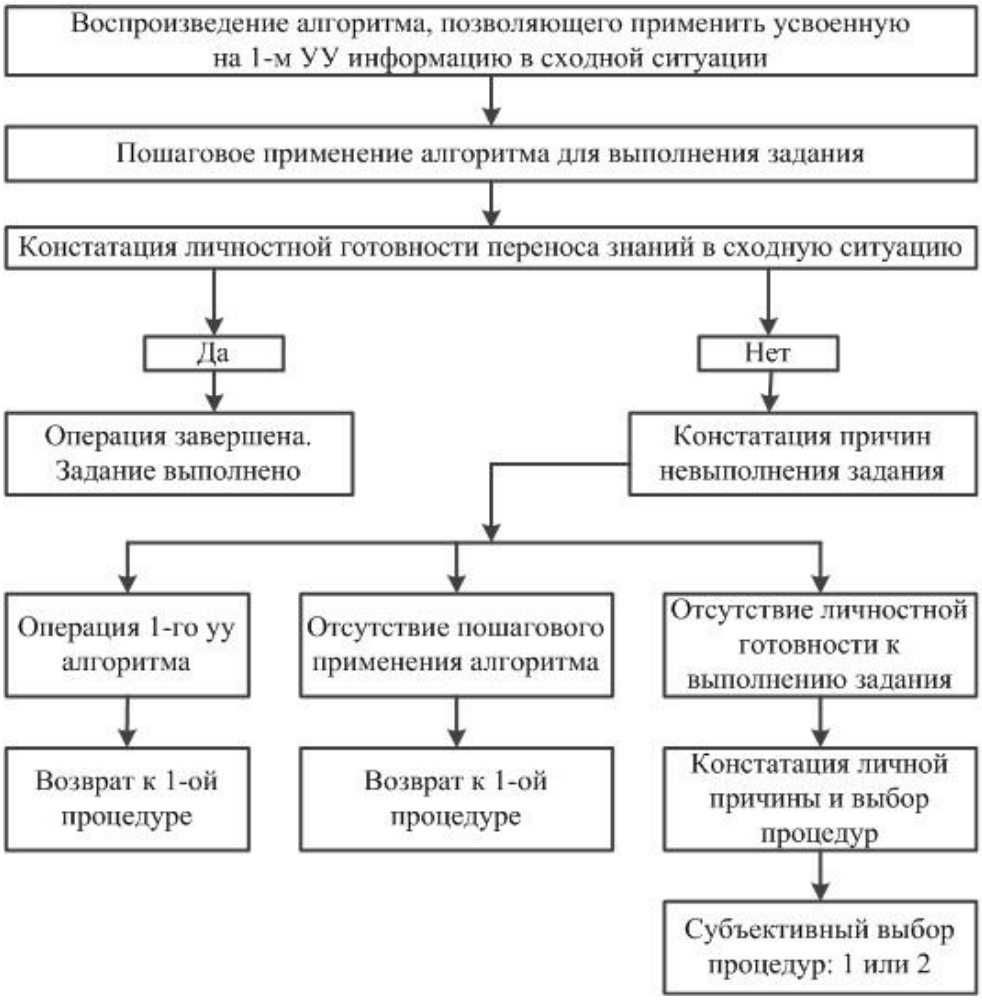


Рисунок 2 – Алгоритм рефлексии содержательно-образовательной цели (2УУ)

Для рефлексии состояния достижения цели усвоения информации на 2-м УУ выполняются следующие процедуры: проверка уровня сформированности у студентов способности к самоанализу, согласно целями обучения, проверка адекватности выбранных технологий достижения. Анализ осуществляется посредством диалога со студентами о том, усвоена ли информация на планируемом уровне. Вместе с тем, важно не то, что педагог фиксирует факт усвоения информации, а то, что студенты, как субъекты учения, учатся осуществлять рефлексию своей деятельности как по усвоению материала темы занятия, так и деятельности в системе обучения.

Аналогично необходимо научить студентов осуществлять рефлексию достижения мировоззренческой цели. Можно предложить последовательность процедур, показанную на рисунке 3. Формирование деятельности по овладению рефлексией осуществляется по этапу цикла управления. Когда отработаны этапы технологии на 2-м УУ, можно переходить к интегративному системному самоанализу.

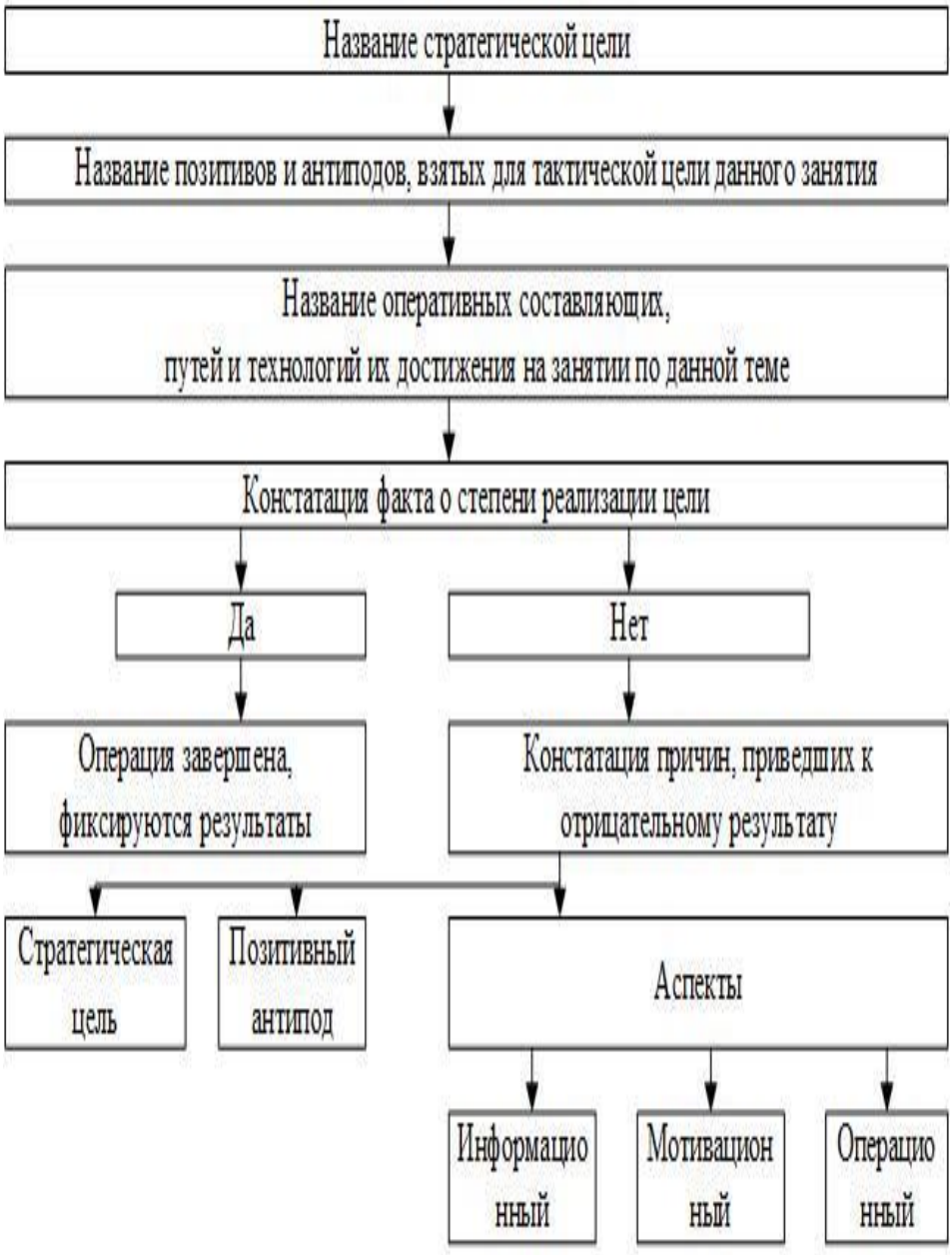


Рисунок 3 – Алгоритм рефлексии мировоззренческой цели

Таким образом, студенты при взаимодействии систем преподавания и учения и предметной области учебной дисциплины овладевают:

- информацией о целях системы обучения на всех уровнях их декомпозиции при репродуктивной деятельности;
- информацией о технологиях обучения;
- алгоритмом принятия решений,
- алгоритмом исследовательской деятельности на репродуктивном и творческом уровнях в учебной деятельности;
- информацией о механизмах моделирования систем и управлении их взаимодействием.

В результате реализации описанных механизмов студенты принимают предметную область знаний как средства своего интеллектуального развития и саморазвития духовно-нравственной культуры за счет фиксации, принятия и организации собственной деятельности на основе целей оперативного уровня и адекватных технологий, осознают себя субъектом и определяют субъектно-субъектные позиции в взаимодействии с другими пользователями, информационными системами и в последующей профессиональной деятельности.

Перечень используемой литературы и источников:

1. Российская Федерация. Президент Российской Федерации. Об утверждении Доктрины информационной безопасности Российской Федерации: Указ Президента РФ от 5 декабря 2016 года № 646 // СПС «КонсультантПлюс».
2. Российская Федерация. Законы. Об информации, информационных технологиях и о защите информации: Федер. закон от 27 июля 2006 года № 149-ФЗ // СПС «КонсультантПлюс».
3. Суханова, С.Г., Дворянкина Е.К. Становление духовно-нравственной культуры будущих инженеров в системе обучения вуза средствами математики: Монография / С.Г. Суханова, Е.К. Дворянкина. – Новосибирск: ФГОБУ ВПО «СибГУТИ», 2011. – 115 с.

ГЛАВА 4.
БИЗНЕС, ЭКОНОМИКА, УПРАВЛЕНИЕ В КОНТЕКСТЕ ОБЕСПЕЧЕНИЯ ИНФОРМАЦИОННОЙ БЕЗОПАСНОСТИ

4.1. АНАЛИЗ ОСНОВНЫХ ОСОБЕННОСТЕЙ ИНФОРМАЦИОННО-ТЕЛЕКОММУНИКАЦИОННЫХ СИСТЕМ ВНУТРИ ПРОИЗВОДСТВЕННЫХ ПРЕДПРИЯТИЙ

В работе представлены требования, которые существуют для информационно-телекоммуникационных сетей внутри предприятий. Рассмотрено множество решений в области информационно-телекоммуникационных сервисов для производственных предприятий. Представлены примеры корпоративных микросервисов для информационно-телекоммуникационных сетей. Рассмотрены особенности сервисов отслеживания ресурсов. Дан анализ технологий, используемых для реализации корпоративных информационно-телекоммуникационных решений. Рассмотрены подходы к автоматизации управления корпоративными задачами в области удаленного обслуживания инцидентов. Показаны возможности облачной платформы управления IT-сервисами.
Ключевые слова: информационно-телекоммуникационная система, ИТ-сервис, компьютерная сеть, производственное предприятие, корпоративный микросервис.

ANALYSIS OF THE MAIN FEATURES OF INFORMATION AND TELECOMMUNICATION SYSTEMS INSIDE PRODUCTION ENTERPRISES

The paper presents the requirements that exist for information and telecommunication networks within enterprises. Many solutions in the field of information and telecommunication services for manufacturing enterprises are considered. Examples of corporate microservices for information and telecommunication networks are presented. The features of resource tracking services are considered. An analysis of the technologies used to implement corporate information and telecommunication solutions is given. Approaches to automating the management of corporate tasks in the field of remote incident servicing are considered. The capabilities of the cloud IT service management platform are shown.
Keywords: information and telecommunication system, IT service, computer network, manufacturing enterprise, corporate microservice.

В XXI веке IT-сервисы становятся полноправным участником бизнеса, выступая в роли посредников между компаниями, людьми, участниками любого производственного, экономического или социального процесса. Выбирая путь постоянного планомерного улучшения качества, оказываемого конечному заказчику сервиса, многие ИТ-компании обращаются за помощью к методологии ITIL (The IT Infrastructure Library). В IT-отрасли, в частности сервисного обслуживания, актуальна задача повышения качества обслуживания конечных пользователей и инфраструктуры заказчика. Если говорить терминами ITIL, то по каждой проблеме конечного пользователя создается сущность, которая называется инцидент, предназначенная для решения компетентной линией поддержки в зависимости от зоны ответственности. Очевидно, что таких инцидентов может быть много, и основной задачей является быстрое реагирование на входящий инцидент, его анализ и правильное назначение на инженера или команду, которые могут и должны решить инцидент в кратчайшие сроки [1]. Помимо этого, человек, который выполняет роль координатора, должен обладать знаниями «Multi-Skill Engineer» («Многопрофильный инженер»), чтобы выявить правильную команду решения, но в реальной ситуации велика субъективность принятия решений. Поэтому необходимо переложить задачи «Incident Coordinator» («Координатора Инцидентов») на компьютерную модель принятия решения. Поскольку в настоящее время IT-обслуживание строится на принципах ITIL методологий, процессы исполнения, координации и управления являются частью функциональной

деятельности.

Информационно-телекоммуникационные системы (ИТС) являются важным элементом управления производственным предприятием. Они позволяют обеспечить связь между всеми участниками производственного процесса, быстро и эффективно передавать информацию, повышать эффективность работы и сократить издержки. На производственном предприятии ИТС включают в себя различные информационные системы, такие как СЭД (система электронного документооборота), СКС (система контроля и управления доступом), СУБД (система управления базами данных), различные микросервисы, ERP (система управления предприятием), WMS (система управления складами) и другие. Внедрение информационно-телекоммуникационных сетей (ИТС) внутри производственных предприятий позволяет:

1. Оптимизировать управление производственными процессами, повысить эффективность системы управления и контроля над бизнес-процессами.

2. Обеспечить прозрачность производственной деятельности и ускорить принятие решений.

3. Повысить уровень автоматизации и упростить работу сотрудников производственного предприятия [2].

4. Сократить время на выполнение производственных операций и уменьшить риски ошибок, связанных с ручными операциями.

5. Повысить качество продукции и улучшить обслуживание клиентов. Таким образом, внедрение ИТС внутри производственных предприятий является необходимым шагом для повышения эффективности работы, уменьшения издержек и улучшения качества продукции. ИТС для крупных производственных предприятий имеют несколько особенностей.

1. Высокая пропускная способность: Крупные производственные предприятия могут иметь большое количество рабочих мест и большой поток информации, которую нужно передавать в ИТС. Поэтому ИТС должна иметь высокую пропускную способность.

2. Надежность: ИТС крупных производственных предприятий должны быть достаточно надежными, чтобы гарантировать непрерывность работы. Надежность может быть достигнута за счет использования резервированных каналов, аварийных источников питания и других технологий.

3. Безопасность: ИТС должна гарантировать безопасность передаваемой информации, потому что крупные производственные предприятия могут иметь большой объем конфиденциальной информации.

4. Управление: ИТС должна быть хорошо управляема и легко конфигурируема, чтобы обеспечить быстрый доступ к информации и оперативное взаимодействие сотрудников.

5. Использование современных технологий: ИТС должна быть построена на современных технологиях, чтобы обеспечивать максимальную эффективность в передаче данных, мониторинге производственных процессов и управлении ресурсами.

6. Интеграция: ИТС крупных производственных предприятий должны быть способны взаимодействовать с другими системами, такими как системы управления производственными процессами, системы управления складом, системы управления ресурсами человеческого потенциала и другие для обеспечения четкой и последовательной передачи данных [3].

Уникальные требования к ИТС зависят от каждого отдельного предприятия и могут отличаться в зависимости от целей и задач, которые стоят перед данной компанией, а также от сферы бизнеса, в которой она работает.

Существует множество решений в области информационно-телекоммуникационных сервисов для производственных предприятий. Ниже представлен обзор нескольких таких решений.

1. SAP ERP – это решение, которое позволяет управлять различными аспектами бизнеса, в том числе производственными процессами, логистикой и продажами. Оно поддерживает автоматизацию и оптимизацию бизнес-процессов, позволяет получать более точную и своевременную информацию в режиме реального времени и улучшает управляемость.

2. Microsoft Dynamics 365 – это решение, которое объединяет в себе ERP и CRM-системы. Оно позволяет управлять всеми деловыми процессами, в том числе управлением производственными процессами. Оно помогает оптимизировать бизнес-процессы, ускорить принятие решений и повысить производительность.

3. Odoo – это бесплатное решение с открытым исходным кодом, которое включает в себя модули управления бухгалтерскими записями, продажами, производственными процессами и другими. Оно позволяет управлять всеми аспектами бизнеса в единой системе.

4. Plex Manufacturing Cloud – это облачное решение, которое предоставляет широкие возможности для управления производством. Оно объединяет в себе ERP, MES (систему управления производственными процессами), CAPM (систему управления отношениями с клиентами), SCM (управление цепочкой поставок) и другие системы. Оно предоставляет возможность автоматизировать производственные процессы, установить контроль над качеством продукции и повысить производительность.

5. Infor CloudSuite Industrial – это облачное решение, которое предназначено для управления производственными процессами. Оно помогает оптимизировать бизнес-процессы, контролировать качество продукции и ускорять принятие решений.

6. QAD Cloud ERP – это облачное решение, которое позволяет управлять всеми аспектами бизнеса, включая производственные процессы. Оно предоставляет возможности для оптимизации производительности, анализа данных, управления качеством продукции и другое. Это только некоторые из примеров решений в области информационно-телекоммуникационных сервисов для производственных предприятий. Каждое решение имеет свои уникальные особенности и возможности, поэтому выбор определенного продукта будет зависеть от потребностей конкретного предприятия [4].

Корпоративные микросервисы – это небольшие и независимые программные компоненты, которые выполняют определенную задачу в рамках ИТС. Каждый микросервис может иметь свой собственный набор баз данных, интерфейсов с другими микросервисами и правилами доступа. Ниже представлены примеры корпоративных микросервисов для ИТС:

1. Сервис отслеживания ресурсов – это микросервис, который отслеживает использование ресурсов, таких как CPU, память и диск, на всех серверах в ИТС. Он позволяет быстро реагировать на проблемы с ресурсами и оптимизировать работу серверов.

2. Сервис управления пользователями – это микросервис, который управляет пользователями в ИТС, такими как создание, изменение и удаление учетных записей, назначение прав доступа и т.д. Он обеспечивает безопасность и защиту данных, контролирует доступ сотрудников к информации и позволяет управлять разрешениями пользователей.

3. Сервис управления журналами – это микросервис, который создает и управляет журналами активности всех компонентов ИТС. Он используется для отслеживания действий пользователей, регистрации ошибок и проблем, связанных с безопасностью.

4. Сервис управления интеграциями – это микросервис, который позволяет интегрировать ИТС с другими приложениями, такими как системы управления клиентами (CRM), электронный документооборот (СЭД) и другие. Он обеспечивает целостность и правильную передачу данных между различными приложениями.

5. Сервис управления заданиями – это микросервис, который управляет выполнением заданий и процессов в ИТС, таких как ежедневное резервное копирование, обновление и тестирование приложений, очистка баз данных и т.д. Он позволяет автоматизировать повторяющиеся задачи и оптимизировать работу ИТС.

Более подробно о сервисах отслеживания ресурсов:

1. Zabbix – это открытое программное обеспечение, которое позволяет отслеживать статус серверов, сетевых устройств, баз данных и других приложений, используя различные протоколы, такие как SNMP, JMX, IPMI и другие. Он предоставляет множество функций, таких как уведомления о проблемах, поиск логических зависимостей, мониторинг производительности и создание отчетов.

2. Nagios – это открытое программное обеспечение, которое позволяет отслеживать статус серверов, сетевых устройств, приложений и других систем. Он может использоваться для мониторинга производительности, мониторинга сетевых устройств, контроля уровня сервиса и автоматического уведомления о проблемах.

3. Datadog – это облачный сервис мониторинга, который позволяет отслеживать статус серверов, контейнеров, приложений и сетевых устройств. Он предоставляет функции мониторинга производительности, анализа данных, оповещения об ошибках и создания отчетов.

4. SolarWinds – это линейка программного обеспечения для мониторинга сети и отслеживания ресурсов, которая включает в себя продукты, такие как: «Network Performance Monitor», «Server & Application Monitor» и другие. Он предоставляет множество функций, таких как мониторинг производительности, мониторинг сетевых устройств, автоматическая отправка оповещений, мониторинг баз данных и другие.

5. PRTG Network Monitor – это программное обеспечение для мониторинга сети, которое позволяет отслеживать состояние серверов, устройств, приложений и сетей в режиме реального времени. Он предоставляет множество функций, таких как мониторинг сетевых устройств, мониторинг производительности, автоматическая отправка оповещений, автоматический поиск устройств и другие.

Это только некоторые примеры сервисов отслеживания ресурсов в ИТ. Каждый продукт имеет свои уникальные особенности и возможности, поэтому выбор конкретного продукта будет зависеть от потребностей конкретного предприятия.

Существует множество технологий, используемых для реализации корпоративных информационно-телекоммуникационных решений. Вот несколько примеров:

1. *Облачные технологии*. Облачные технологии предоставляют возможность использования вычислительных мощностей и хранения данных на удаленных серверах, что может сократить затраты на ЦОД и обеспечить масштабируемость и гибкость системы.

2. *Виртуализация*. Виртуализация позволяет создавать виртуальные экземпляры операционных систем, приложений и баз данных, что может сократить затраты на инфраструктуру и обеспечить гибкость и масштабируемость системы.

3. *Интернет вещей* (IoT). Технологии IoT могут быть использованы для создания информационно-телекоммуникационных решений для мониторинга состояния оборудования и процессов на производстве, автоматизации процессов и сбора данных.

4. *Большие данные* (Big Data). Технологии Big Data позволяют анализировать большие объемы данных, собранных с различных источников, таких как датчики, устройства IoT, системы управления производственными процессами, CRM системы и другие.

5. *Искусственный интеллект* (AI). Технологии AI могут быть использованы для анализа и обработки больших объемов данных, автоматизации рутинных задач и управления рисками.

6. *SDN* (Software-Defined Networking). Технология SDN используется в компьютерных сетях для централизованного управления сетью с помощью программного обеспечения, что позволяет улучшить управляемость и гибкость сети.

7. *DevOps и Agile*. Методологии разработки и управления проектами, такие как «DevOps» и «Agile», могут быть использованы для обеспечения гибкости и быстрого внедрения корпоративных информационно-телекоммуникационных решений.

Кроме того, каждое конкретное решение могут быть реализовано с использованием различных комбинаций технологий в зависимости от его целей, требований и возможностей.

«Software-Defined Networking» (SDN) является методологией управления сетями, которая позволяет пользователям автоматизировать и программировать устройства сети. Она также упрощает назначение и управление трафиком в сети, что позволяет быстро настраивать, обеспечивать безопасность и оптимизировать работу сети. В этом обзоре мы рассмотрим ряд решений в области SDN.

1 «Application Centric Infrastructure» (Cisco ACI): ACI является решением SDN, разработанным Cisco. Оно предназначено для управления сетевым трафиком, построенным на базе концепции центра приложений. ACI позволяет управлять сетью центра приложений, используя единую точку управления и автоматические механизмы конфигурации. Он также обеспечивает возможности масштабирования, безопасности и мониторинга сети.

2. VMware NSX: NSX – это SDN-решение от VMware, которое предоставляет виртуальное управление виртуальными серверами и сетями, не зависящее от физической аппаратной инфраструктуры. NSX позволяет управлять трафиком, настраивать сетевые подключения и назначать правила безопасности, используя визуальный интерфейс. Он также обеспечивает масштабирование и управление виртуальными сетями.

3. Juniper Contrail («Contrail») является SDN-решением от компании Juniper Networks, которое предоставляет программное управление всеми сетевыми ресурсами. Эта платформа имеет интеллектуальный контроль трафика и гибкую настройку контроллеров, что обеспечивает управление сетью на разных уровнях. Contrail также поддерживает многочисленные сетевые технологии и является открытым программным обеспечением.

4. OpenDaylight – это SDN-платформа с открытым исходным кодом, поддерживаемая «Linux Foundation». Она предоставляет основы для разработки новых программных приложений SDN. Это позволяет пользователям создавать новые решения, основанные на SDN, для конкретных задач, таких как управление сетевой сегментацией, настройка политик маршрутизации и управление безопасностью. Все перечисленные выше SDN-решения предоставляют множество преимуществ для пользователей, в том числе возможность автоматизации и программирования устройств сети, упрощение настройки трафика, повышение безопасности и масштабирования, а также упрощение управления, мониторинга и отладки. Реализация SDN-решений может значительно улучшить работу сети и повысить удовлетворенность пользователей.

Существует несколько подходов к автоматизации управления корпоративными задачами в области удаленного обслуживания инцидентов. Рассмотрим некоторые из них:

1. Автоматизированные системы управления заявками и запросами (ITSM) – эти системы помогают управлять возникшими проблемами и инцидентами в компании, позволяя автоматически распределять задачи и контролировать выполнение работ по решению проблем.

2. Мониторинг и управление инцидентами – Мониторинг инцидентов происходит в режиме реального времени и позволяет оперативно принимать решения о

приоритетах и эскалации заявок на решение проблем.

3. Использование систем ИИ и машинного обучения – эти системы позволяют в автоматическом режиме анализировать данные, обрабатывать заявки и давать конкретные рекомендации по решению проблем в режиме реального времени.

4. Роботизированный процесс автоматизации (RPA) – эта технология позволяет автоматизировать рутинные задачи, такие как формирование отчетности, просмотр и анализ данных и другие задачи, которые не требуют участия человека.

5. Использование средств аналитики данных для выявления тенденций в работе, идентификации узких мест в процессах управления инцидентами и разработке эффективных стратегий управления производительностью. Каждый из этих подходов имеет свои плюсы и минусы и может быть наиболее эффективным в зависимости от ситуации, бюджета и других факторов. В любом случае, автоматизация управления корпоративными задачами может значительно повысить эффективность и точность процессов управления инцидентами в компании.

Автоматизированные системы управления заявками и запросами (ITSM) – это программное обеспечение, которое управляет процессами поддержки клиентов, в том числе управляет инцидентами, проблемами, изменениями и уровнями обслуживания. [5,6] Эти системы позволяют организациям управлять своими IT-ресурсами и процессами, используя стандарты бест-практик, такие как ITIL («Information Technology Infrastructure Library»). ITSM-системы включают в себя широкий спектр функций, которые помогают управлять заявками на поддержку, проактивно предупреждать возможные проблемы, автоматизировать процессы и анализировать данные:

1. Управление инцидентами – эта функция позволяет регистрировать заявки на решение проблем и управлять ими вплоть до их закрытия.

2. Управление проблемами – данная функция позволяет выявлять причины возникновения проблем и предотвращать их повторное возникновение.

3. Управление изменениями – это функция, которая позволяет управлять изменениями в IT-среде, отслеживать их выполнение и вносить коррективы, если это необходимо.

4. Управление уровнями обслуживания – эта функция позволяет определять уровни обслуживания в соответствии с потребностями клиента, а также отслеживать выполнение обязательств перед клиентами.

5. Управление конфигурациями – это функция, которая позволяет управлять конфигурациями IT-среды и отслеживать изменения, произведенные в ней [7, 8].

6. Управление активами – данная функция позволяет управлять активами и ресурсами компании, включая компьютеры, сервера, принтеры и другие устройства и программное обеспечение.

ITSM-системы могут быть настроены под определенные бизнес-потребности и могут работать как локально, так и по сети. Важным аспектом автоматизации управления заявками и запросами является возможность анализировать данные и выявлять области для улучшения производительности и качества обслуживания клиентов. Некоторые из популярных ITSM-систем включают в себя: «Jira Service Desk», «ServiceNow», «Zendesk», «Freshservice» и «Zoho Desk». Они предлагают ряд различных функций и интеграций для удобства управления заявками и запросами.

«Jira Service Desk» – это программное обеспечение для управления заявками и запросами, которое обеспечивает прозрачность и контроль над IT-сервисами. Позволяет создавать порталы самообслуживания и оптимизировать процессы поддержки клиентов. Среди основных функций «Jira Service Desk» можно выделить:

- Система управления заявками. Позволяет создавать, отслеживать и управлять заявками на поддержку, в том числе инцидентами, запросами и изменениями.

- Система автоматизации. Автоматизирует процессы IT-сервисов, связанных с

заявками.

- Система управления уровнем обслуживания. Позволяет определить уровни обслуживания для каждого клиента или группы клиентов, назначить сотрудника, ответственного за заявку, и установить сроки реакции.

- Система управления базой знаний. Встроенная база знаний, которая может быть использована для предоставления ответов на часто задаваемые вопросы, составления инструкций для решения определенных проблем.

- Система отчетности и аналитики. Позволяет создавать отчеты и анализировать оценки качества обслуживания, просматривать детальные статистические данные о том, какие типы заявок получаются чаще всего. «Jira Service Desk» (Служба поддержки Jira) предоставляет функцию конфигурации страницы портала сервиса. Можно настроить страницы в соответствии с дизайном компании, добавить полезную информацию для пользователей, управлять уровнями доступа к различным разделам страницы.

«ServiceNow» – это облачная платформа управления IT-сервисами, которая объединяет различные IT-системы и процессы для ускорения работы и улучшения качества обслуживания. Среди основных функций ServiceNow можно выделить:

1. Управление заявками на обслуживание. «ServiceNow» позволяет создавать, отслеживать и управлять заявками на обслуживание, включая запросы, инциденты, проблемы и изменения.

2. Управление уровнем обслуживания. «ServiceNow» позволяет определить стандарты обслуживания и интегрировать их в работу компании.

3. Автоматизация процессов. «ServiceNow» позволяет автоматизировать выполнение задач, таких как назначение задач, уведомления и проведение тестирования, что ускоряет процесс обработки заявок.

4. Управление активами и конфигурацией. «ServiceNow» позволяет управлять активами и конфигурациями IT-систем и отслеживать изменения, вносимые в них.

5. Управление базой знаний. Встроенная база знаний, которая может быть использована для предоставления ответов на часто задаваемые вопросы и инструкций для решения определенных проблем.

6. Система отчетности и аналитики. ServiceNow предоставляет возможность создавать отчеты и анализировать оценки качества обслуживания, а также просматривать детальные статистические данные.

Таким образом, представленные подходы дают возможности для того, чтобы осуществлять повышение эффективности работы производственных предприятий. Дан анализ особенностей сервисов отслеживания ресурсов. На основе большого числа решений в информационно-телекоммуникационных сетях можно реализовывать процессы автоматизации. Продемонстрированы и показаны возможности облачной платформы управления IT-сервисами.

Перечень используемой литературы и источников:

1. Преображенский Ю.П., Паневин Р.Ю. Формулировка и классификация задач оптимального управления производственными объектами // Вестник Воронежского государственного технического университета. – 2010. Т. 6. № 5. – С. 99-102.

2. Львович И.Я., Преображенский А.П., Чопоров О.Н. Использование информационных систем в управлении производством // Научный взгляд в будущее. – 2018. Т. 3. № 9. – С. 94-98.

3.Черников С.Ю., Корольков Р.В. Использование системного анализа при управлении организациями // Моделирование, оптимизация и информационные технологии. – 2014. - № 2 (5). – С. 16.

4. Преображенский Ю.П., Коновалов В.М. О методах создания рекомендательных систем // Вестник Воронежского института высоких технологий. – 2019. - № 4 (31). – С. 75-79.

5. Львович И.Я., Преображенский А.П., Преображенский Ю.П., Чопоров О.Н. Проблемы использования технологий интернет вещей // Вестник Воронежского института высоких технологий. – 2019. - № 1 (28). – С. 73-75.

6. Гостева Н.Н., Гусев А.В. О возможности увеличения эффективности производства // Вестник Воронежского института высоких технологий. – 2017. - № 1 (20). –С. 76-78.

7. Преображенский Ю.П., Мясников О.А. Анализ перспектив информационных технологий в сфере

интернет вещей // Вестник Воронежского института высоких технологий. – 2020. - № 1 (32). – С. 43-45.
8. Жилина А.А., Кострова В.Н., Преображенский Ю.П. Разработка методики постановки задачи выбора управленческого решения на основе оптимизационного подхода // Моделирование, оптимизация и информационные технологии. – 2018. Т. 6. № 1 (20). – С. 243-253.

4.2. ПЕРСПЕКТИВЫ ПРИМЕНЕНИЯ ЦИФРОВЫХ ТЕХНОЛОГИЙ В ОРГАНИЗАЦИОННЫХ И ФУНКЦИОНАЛЬНЫХ МЕХАНИЗМАХ ЭКОНОМИЧЕСКОЙ И ПРАВОВОЙ СИСТЕМ РОССИИ В ЦЕЛЯХ ОБЕСПЕЧЕНИЯ ИНФОРМАЦИОННОЙ БЕЗОПАСНОСТИ В УСЛОВИЯХ НЕОПРЕДЕЛЕННОСТИ

В работе исследуются нормативно-организационные и технологические аспекты реализации высоких (цифровых) технологий в обеспечении информационной и комплексной безопасности экономической и правовой систем России в современный период.
Проведен сопоставительный анализ определений и особенностей реализации процессов цифровизации и цифровой трансформации, определены наиболее важные проблемы цифровизации и цифровой трансформации в стране, обозначены основные тенденции развития в сфере цифровизации и цифровой трансформации применительно к экономической и правовой системам в ближайшие годы.
Сделан вывод, что в современный период, в условиях допущения состояния неопределенности и возникающих рисков внешнего воздействия применения цифровых технологий в системах управления и функционирования организационных систем оправдано с точки зрения повышения конкурентоспособности, необходимости обеспечения комплексной безопасности, устойчивости функционирования систем, а также необходимым условием выживания.
Ключевые слова: государство, информационная, комплексная безопасность, правовая система, развитие, управление, цифровая трансформация, цифровизация, экономическая система, эффективность.

PROSPECTS FOR THE APPLICATION OF DIGITAL TECHNOLOGIES IN ORGANIZATIONAL AND FUNCTIONAL MECHANISMS OF THE ECONOMIC AND LEGAL SYSTEMS OF RUSSIA FOR THE PURPOSES OF ENSURING INFORMATION SECURITY IN CONDITIONS OF UNCERTAINTY

The work examines the regulatory, organizational and technological aspects of the implementation of high (digital) technologies in ensuring information and comprehensive security of the economic and legal systems of Russia in the modern period. A comparative analysis of definitions and features of the implementation of digitalization and digital transformation processes was carried out, the most important problems of digitalization and digital transformation in the country were identified, and the main development trends in the field of digitalization and digital transformation in relation to economic and legal systems in the coming years were identified. It is concluded that in the modern period, under the assumption of a state of uncertainty and emerging risks of external influence, the use of digital technologies in management systems and the functioning of organizational systems is justified from the point of view of increasing competitiveness, the need to ensure comprehensive security, the sustainability of the functioning of systems, as well as a necessary condition for survival.
Keywords: state, information, comprehensive security, legal system, development, management, digital transformation, digitalization, economic system, efficiency.

Актуальность рассмотрения вопроса. Современное развитие общества и государства для многих из нас не является четко определенным, поскольку сегодня не до конца определены и оценены уровни внешних и внутренних угроз. Мы не знаем, какой фактор внешнего или внутреннего воздействия на государство или на его отдельные системы и институты является определяющим, но мы точно знаем, что любое воздействие извне приводит к определенному отклику.

Сложившаяся сегодня в мире острая геополитическая обстановка, попирание всех норм международного права и фактическое отсутствие гарантий для соблюдения

права собственности со стороны коллективного Запада (это мы видим на примере замороженных или конфискованных активов России, российских юридических и физических лиц недружественными странами Запада), необъективность при принятии решений международными организациями (включая ООН, МАГАТЭ, ПАСЕ), наконец, вторжение в информационную сферу деятельности российского государства – представляют собой явную угрозу национальной безопасности России, что, в свою очередь, привело к относительно вынужденной, но правильной и необходимой смене (а точнее, корректировке) курса развития российской государственности, в том числе, в сфере обеспечения безопасности всех подсистем, начиная от правовой и заканчивая информационной. Указанная практика деятельности является комплексной [1, с. 85].

Необходимость проведения анализа проблематики обеспечения безопасности систем определяется тем, что в настоящее время функционирование всех систем Российской Федерации зависит от воздействия внешних и внутренних факторов, причём воздействие внешней среды, с нашей точки зрения, характеризуется неопределённостью, обеспеченной флуктуационной внешнеполитической мировой ситуацией, отсутствием закономерных правил поведения внешнеэкономических систем, нарушением норм международного права со стороны недружественных зарубежных контрагентов и вовлечением в общемировое экономическое, правовое и политическое пространство политики двойных стандартов. С другой стороны, многие социально-экономические (и правовые) системы сами характеризуются высокой степенью неопределенности, источниками которой являются экономические и управленческие факторы [2].

С учетом изложенного, достаточно важным и полезным для изучения становится именно проблематика дальнейшего развития основных систем жизнеобеспечения, в первую очередь, экономическую (хозяйственную) и правовую, которые в большинстве своем находятся в тесном взаимодействии, включая высокотехнологичные, цифровые сферы, развитие IT-технологий, структур ВПК. В настоящей работе в качестве объекта исследования мы определяем не нечто абстрактное, а конкретные субъекты хозяйственной и правовой деятельности (организации коммерческие и некоммерческие, учреждения, институты, саму экономическую и правовую системы, как на федеральном, так и на региональном уровнях).

Рассматривая в целом вопросы обеспечения безопасности, механизмом ее реализации применительно к любой системе является деятельность органов управления системы и ее субъектов по выявлению, предупреждению угроз безопасности системе и противодействию им в качестве обязательного и непрерывного условия защиты корпоративных интересов. Сущность этой деятельности определяется политикой обеспечения безопасности, формулируемой органами управления [3, с.88].

В свою очередь защита от негативной информации состоит в применении определенных методов и средств защиты от негативного влияния на составляющие какой-либо системы информации, как внутренней, так и поступающей извне.

На наш взгляд, проблема защиты от информационных угроз гораздо серьезнее проблемы защиты информации, т.к. воздействие этих угроз, как правило, трудно выявить, т.е. они не всегда очевидны [4]. Помимо этого, защита от информационных угроз требует скорее не технических решений, а, в первую очередь, решений организационного и правового характера.

Оценка оптимального поведения экономической и правовой системы в современных условиях с позиций инновационного развития и обеспечения комплексной безопасности. Постоянный рост темпов развития и распространения информационных технологий, высокая конкуренция и существующая криминогенная обстановка ставят вопрос о создании внутри системы и ее структурных элементов единой, соответствующей всем современным требованиям системы или подсистемы информационной безопасности. Система обеспечения информационной безопасности

должна включать и увязывать в себе правовые, организационные, физические, инженерно-технические и программные направления обеспечения защиты информационных ресурсов, и сама должна быть включена в общую систему обеспечения безопасности системы. При этом, как отмечают исследователи задачами политики информационной безопасности выступают выбор оптимального способа использования информационных ресурсов, а также разработка процедур, предотвращающих или реагирующих на нарушения режима безопасности [5].

Стабильность функционирования государственных институтов, спокойное развитие гражданского общества, уверенность граждан в завтрашнем дне, мирная внешнеполитическая обстановка – вот те краеугольные элементы системы, которую принято называть элементами обеспечения комплексной безопасности.

Под безопасностью понимается состояние и условия жизнедеятельности социума, его систем, структур, институтов и установлений, при которых обеспечивается сохранение их качественной определенности с объективно обусловленными инновациями в ней и свободное, соответствующее собственной природе и ею определяемое функционирование при исключении или нейтрализации возможности причинения им какого-либо ущерба, вреда либо придания развитию нежелательных динамики или параметров [6].

В России на сегодня действительно много проблем, которые в совокупности образуют угрозы комплексной безопасности государства и его подсистем. В этой части, рассуждая о проблемах комплексной безопасности, необходимо вести речь о необходимых мерах, направленных на ее обеспечение и на минимизацию возникающих извне и внутри угроз.

Важнейшим элементом укрепления безопасности страны является обеспечение законности, построение правового государства, повышение доверия населения к правоохранительной, судебной системам, создание действенных институтов, способных реально обеспечить защиту прав и свобод граждан и законных интересов хозяйствующих субъектов.

Сегодня, можно лишь с уверенностью констатировать, что обеспечение комплексной безопасности государства возможно лишь при правильном определении потенциальных и реальных угроз, подборе и согласовании функциональных целей и методов их нейтрализации или минимизации, а также при условии единства согласованных целей и действий всех элементов указанной системы.

Управленческие решения в области обеспечения информационной безопасности экономической и правовой систем с ориентацией на экономическую стабильность и устойчивость системы. Цифровизация и цифровая трансформация систем. Под обеспечением безопасности системы следует понимать целенаправленную деятельность всех ее элементов (подсистем), включая подсистемы управления по выявлению, предупреждению всех имеющихся угроз безопасности хозяйствующего субъекта (правовых, информационных, экономических, технологических и др.) и противодействию им в качестве обязательного и непрерывного условия защиты интересов субъекта.

В системном анализе и синтезе устойчивость используется в комплексе интегральных характеристик сложного объекта, отражающих его взаимодействие со средой, внутреннюю структуру и поведение, и является одним из первичных качеств любой системы. В общем смысле под устойчивостью понимается способность системы сохранять некоторое ее свойство по отношению к возмущению или неопределенности некоторых параметров самой системы или внешней среды. Устойчивость во взаимосвязи с другими первичными качествами системы способствует ее эффективности, что, в конечном счете, формирует безопасность системы.

Не вдаваясь в подробности анализа механизма принятия решения, направленного на обеспечение информационной безопасности, отметим, что основная

роль в принятии решения должна отводиться специальным субъектам управления, напрямую имеющим отношение к соответствующей сфере противодействию угроз. При этом определяющую роль в принятии необходимого решения, с нашей точки зрения, играет фактор законности, который во многом зависит от профессионального уровня субъекта, принимающего решение. Итоговое управленческое решение по обеспечению информационной безопасности должно носить законный характер и опираться на исключительно правомерные действия.

Обратимся к терминологии. Цифровизация – это внедрение цифровых технологий и систем с перестройкой организационных и функциональных (бизнес-процессов) по принципам бережливого производства и повышением эффективности, созданием гибкости. Также это начало работы с данными и принятия решений на их основе. Характеризуется снижением внутренних издержек и повышением эффективности, получением конкурентных преимуществ в рамках существующей функциональной бизнес-модели.

Примеры технологий и решений цифровизации: внедрение ERP, интеграция систем, облачные технологии, использование «SaaS», «PaaS» и «IaaS» для организации работы, переход на использование безбумажных технологий, ЭЦП, использование технологий блокчейна и т.д.

Основные компоненты цифровизации системы включают в себя:

- Цифровые сервисы (цифровая платформа, информационные системы, личные кабинеты, интеграция и безопасность);
- Информационные системы (электронный документооборот, управление функциональным процессом);
- Инфраструктура (модернизация материально технического обеспечения (МТО), развитие средств передачи функционального контента);
- Управление данными (организация метаданных и моделей данных, комплексная защита данных);
- Кадры (обучение, повышение квалификации, развитие ИТ-компетенций).

Цифровая трансформация – это глобальная перестройка процессов и системы управления с использованием результатов цифровизации. Она характеризуется:

- кратным снижением издержек на обработку информации (получение, передача, обработка, аналитика);
- изменением организационной структуры, функций, культуры;
- созданием новых продуктов и бизнес-моделей;
- активным использованием сквозной кросс-аналитики для принятия решений;
- цифровыми каналами связи с заинтересованными сторонами;
- разработкой и тестированием на основе данных гипотез и новых продуктов/технологий.

Обратим внимание, что ряд ученых не разделяют цифровизацию и цифровую трансформацию и под цифровой трансформацией понимают процесс интеграции, внедрения и проникновения цифровых технологий во все аспекты жизни общества, которые требуют коренных изменений технологий создания новых продуктов и услуг, изменения культуры социально-экономических отношений, проводимых изменений и принципов построения новых моделей государства и бизнеса [7]. Данный подход с нашей точки зрения может быть оправдан с нашей точки зрения недостаточностью развития высоких технологий в нашей стране и фактическим размытием указанных процессов.

В целом, более правильным будет разграничение понятия «цифровая трансформация» и «цифровизация», которые часто отождествляются. Цифровизация – это социально-экономический процесс, который предшествует цифровой трансформации и заключается в создании базы для нее. Как отмечают исследователи, цифровизация предполагает внедрение информационных систем, и ставят перед

менеджментом системы ряд задач, в том числе, необходимость автоматизации процессов внутреннего контроля, как инструмент обеспечения информационной безопасности системы [8].

Несмотря на определенные успехи в технологичном развитии государства, события последних лет, включая пандемию коронавируса «Covid-19», давшей серьезный импульс в развитии высоких технологий, серьезное санкционное давление недружественных государств, а также проведение специальной военной операции (также активизировавшей применение цифровых инструментов в самых разных областях жизнедеятельности) лишь обострили ситуацию, связанную с недостаточностью и низкими темпами применения цифровых технологий. В этой связи Президент России в Послании Федеральному Собранию 2023 года дополнительно конкретизирует поставленную задачу и заявляет о необходимости «с учетом масштабных задач, стоящих перед страной серьезно обновить подходы к системе подготовки кадров, к научно-технологической политике.

Отметим, что основная задача анализируемых систем России заключается в их надлежащем функционировании в целях обеспечения экономической и социальной стабильности, правопорядка и законности, а также в целях надлежащего обеспечения прав, свобод и безопасности граждан. Вполне очевидно, что выполнение данных задач напрямую связано с повышением управляемости правовой и экономической системой, эффективности информационного обмена как внутри систем, так и во взаимодействии между собой, с иными системами, государственными органами и учреждениями, а также во взаимодействии с институтами гражданского общества, что, в свою очередь потребует развитие информационного и телекоммуникационного обеспечения, своего рода цифровой трансформации.

Обозначим наиболее важные проблемы цифровизации и цифровой трансформации применительно к анализируемым системам:

- Не разработаны и не внедрены нотации функциональных бизнес-процессов, они не взаимоувязаны с функциональной структурой систем;
- Недостаточно развиты онлайн-курсы практико-ориентированного классического образования и ДПО, нет интеграции с «большими внешними системами» (образовательная, цифровая);
- Не внедрена ERP-система или её компоненты (стратегия интеграции производства и операций, управления трудовыми ресурсами, финансового менеджмента и управления активами, ориентированная на непрерывную балансировку и оптимизацию ресурсов предприятия посредством специализированного интегрированного пакета прикладного программного обеспечения, обеспечивающего общую модель данных и процессов для всех сфер деятельности);
- Отсутствие необходимого количества профессиональных сотрудников, отвечающих за проведение цифровизации систем;
- Не разработана и не сформирована необходимая нормативно-правовая база, которая служит фундаментом и для любых изменений в стратегии развития государства, в том числе в реализации цифровой трансформации [9].

Какие же основные перспективы в сфере цифровизации и цифровой трансформации ожидают нас в ближайшие годы:

- Внедрение отечественных ВКС-платформ («Сферум» и др.);
- Усиление импортозамещения в части программного обеспечения;
- Подготовка к переходу на Linux-решения;
- Развитие «единой шины данных» для корпоративных информационных систем;
- Организация обучения специалистов систем, формирование «команд цифровизации» для элементов (субъектов) систем;
- Инвентаризация инфраструктуры, приведение технологий и платформ систем к единым стандартам [10].

Немаловажным направлением применения цифровых технологий в анализируемых системах является применение внутренних информационных систем, по аналогии с корпоративными информационными система (далее - КИС) обычных систем. Подобные системы уже активно функционируют в самых разных сферах, например, КИС Минстроя, КИС «ГАС Правосудие» (судебная система), КИС «ФРДО» (образование), КИС Министерства юстиции, КИС ФССП (система судебных приставов), КИС нотариальной системы, в стадии принятия находится законопроект о КИС адвокатуры и т.д. Особенности нормативного регулирования вопросов формирования подобных информационных систем и их применения возможно сегодня только при наличии множественных нормативных, организационных и технологических связок, позволяющих обеспечивать слаженную работу всех элементов системы. В противном случае нарушается не только правовая основа, но и информационная целостность и происходят сбои в обеспечении субъектов системы точными и актуальными данными.

Немаловажной проблемой, связанной с перспективами применения цифровых технологий в системах, является вопрос обеспечения и защиты персональных данных, как сотрудников, так и осужденных, поскольку действующее законодательство предъявляет достаточно жесткие требования к вопросам обработки и в особенности, распространения персональных данных, влекущие серьезные санкционные последствия. В этом случае достаточно эффективным инструментом будет выступать развитие систем кибербезопасности, введение требований к шифрованию и обезличиванию информации.

Выводы: По результатам работы считаем необходимым сделать следующие выводы.

1. С учетом Посланий Президента России Федеральному Собранию России центральное место в обеспечении информационной безопасности анализируемых систем отводится реализации механизмов цифровизации, т.е. внедрению цифровых технологий в деятельность систем, а также цифровой трансформации, т.е. глобальной перестройке процессов и системы управления с использованием результатов цифровизации. Указанное направление внедрения цифровых технологий во всех сферах жизнедеятельности определено, как важнейшее условие прорывного развития страны.

2. Необходимость применения цифровых технологий в правовой и экономической системах на современном этапе обусловлена тенденциями осуществления информационной открытости, как основных государственных систем, так и ростом объема данных и иной информации, используемой в работе систем, корректировки практико-ориентированной составляющей при формировании кадровых интеллектуальных ресурсов, необходимостью обеспечения комплексной безопасности систем, ориентированием на наиболее эффективные стандарты функционирования аналогичных систем, внедрением и активным использованием дистанционных технологий, повышением роли информации и процессов ее обращения в реализации правоохранительных функций систем и борьбы с коррупцией в системах.

3. Наиболее важными условиями, определяющими эффективность обеспечения информационной безопасности правовой и экономической систем применительно к реализации механизмов цифровизации и цифровой трансформации являются:

- оптимизация системы управления систем;
- совершенствование нормативной базы, регулирующей использование цифровых (информационных) технологий в деятельности систем и ее составляющих, что является важным аспектом для успешного применения цифровых технологий.

4. Обеспечение информационной безопасности в правовой и экономической системах является наиболее перспективным направлением применения цифровых

технологий, которые позволяют реализовать наиболее эффективное взаимодействие систем и их органов управления.

5. Основное внимание при реализации цифровых технологий в деятельности в правовой и экономической системах должно уделяться:

- проблемам обучения, подготовки, переподготовки кадров, задействованных в вопросах цифровизации;

- формированию внутри систем корпоративных информационных систем с элементами обеспечения информационной безопасности;

- повышению управляемости системами эффективности информационного обмена как внутри систем, так и во взаимодействии с иными системами, государственными органами и учреждениями, а также во взаимодействии с институтами гражданского общества;

6. Тенденции в сфере цифровизации и цифровой трансформации в ближайшие годы сводятся к следующим:

- внедрение отечественных ВКС-платформ («Сферум» и др.);

- усиление импортозамещения в части программного обеспечения;

- подготовка к переходу на Linux-решения;

- развитие «единой шины данных» для корпоративных информационных систем;

- организация обучения специалистов систем, формирование «команд цифровизации» для элементов (субъектов) систем;

- инвентаризация инфраструктуры, приведение технологий и платформ систем к единым стандартам.

7. Основополагающим условием эффективного применения цифровых технологий в организационных и функциональных механизмах экономической и правовой системы России в целях обеспечения информационной и комплексной безопасности является формирование необходимой законодательной базы, регламентирующей, в том числе, отношения в сфере принятий решений организационного и технологического характера.

Список используемой литературы и источников

1. Исследования по безопасности / [под ред. С.П. Никанорова] 2-е изд. – Москва: Концепт, 2006. – 624 с.
2. Саткалиева Т.С. Управление социально-экономическими системами в условиях неопределенности / Т.С. Саткалиева, Г.А. Таспенова // Вестник университета. – 2013. - № 7. – С. 210-216.
3. Зыблев В.Б. Правовое обеспечение борьбы с основными угрозами безопасности хозяйствующих субъектов Российской Федерации: дис. …канд. юрид. наук: 12.00.11. – Москва: РАГС, 2006. – 159 с.
4. Воронов А.А. Обеспечение информационной безопасности организации, как необходимое условие ее успешного функционирования / А.А. Воронов, И.Я., Львович, А.В. Багрянцев // Информация и безопасность. – 2005. - № 1. – С. 36-43.
5. Казакова А.В. Концепция информационной безопасности промышленных предприятий / А.В. Казакова// Вестник Самарского государственного университета. – 2011. - № 3 (84). – С. 128-135.
6. Бельков О.А. Понятийно-категориальный аппарат концепции национальной безопасности / О.А. Бельков // Безопасность: Информационный сборник Фонда национальной и международной безопасности. – 1994. – № 3. – С. 91-94.
7. Удалов Д.В. Цифровая трансформация социально-экономического пространства / Д.В. Удалов // Вестник СГСЭУ. – 2020. - № 3 (82). – С. 33-36.
8. Агеева О.А. Специфика обеспечения экономической безопасности в условиях цифровизации / О.А. Агеева О.А., Н.К. Кучукова Н.К., Ю.Д. Матыцына Ю.Д. // Вестник ГГУ. – 2022. - № 4. – С. 100-106.
9. Козырь Н.С. Актуальные проблемы цифровизации социально-экономических систем / Н.С. Козырь // Вестник университета. – 2022. - № 7. – С. 54-59.
10. Одинцова М.А. Тенденции в управлении информационными технологиями / М.А. Одинцова // Вестник Российского нового университета. Серия: сложные системы: модели, анализ и управление. – 2021. - № 1. – С. 61-69.

4.3. АНАЛИЗ ОЦЕНКИ РИСКА «УТЕЧЕК» КОНФИДЕНЦИАЛЬНЫХ ДАННЫХ ПРИ УДАЛЁННОЙ РАБОТЕ В 2018-2020 годах

Статья посвящена анализу влияния дистанционного режима работы на колебания рисков, связанных с угрозой потери информации. В результате исследования выявлено различное воздействие удалённой работы на возможные утечки информации в России и в мире.
Ключевые слова: аутентификация и идентификация, дистанционная работа, информационная безопасность (ИБ), информационные риски, риски, удалённая работа, утечка данных.

ANALYSIS OF THE RISK OF "LEAKS" OF CONFIDENTIAL DATA DURING REMOTE WORK IN 2018-2020

The article is devoted to the analysis of the influence of remote operation mode on fluctuations in risks associated with the threat of information loss. As a result of the study, various effects of remote work on possible information leaks in Russia and in the world were revealed.
Keywords: authentication and identification, remote work, information security (IS), information risks, risks, remote work, data leakage.

В последние несколько лет огромное влияние на реализацию многих процессов оказала пандемия «Covid-19». Исключением не стала и сфера защиты информации на предприятиях. У разного рода компаний стали выявляться новые риски, которые были бы связаны с удалённой работой, одновременно с этим большое давление оказывали действия хакерских группировок. Как следствие, за последние несколько лет произошел резкий рост доли утечек, носящих умышленный характер, а также выросло количество утечек из-за вредительства внешних киберпреступников и пользователей с привилегированными правами доступа.

Ещё в 2016 году в указе Президента РФ «Об утверждении Доктрины информационной безопасности Российской Федерации» утверждается, что «Информационные технологии приобрели глобальный трансграничный характер и стали неотъемлемой частью всех сфер деятельности личности, общества и государства. Их эффективное применение является фактором ускорения экономического развития государства и формирования информационного общества» [6]. Спустя 8 лет активного развития общества и технологий это влияние возросло в разы.

В 2020 году самым заметным событием во всем мире стала пандемия вируса «COVID-19», борьба с которым значительно повлияла на все основные процессы, в результате чего изменились привычные способы предоставления услуг.

Говоря об удалённой работе, стоит отметить тот факт, что число людей, работающих в дистанционном режиме, постоянно росло даже в периоде до 2019 года, хотя условия пандемии, безусловно, ускорили этот процесс. Начиная с 2020 года, который пришёлся на активное применение режима «локдаун», дистанционный рабочий режим зарекомендовал себя как необходимый элемент для обеспечения непрерывной рабочей деятельности любого предприятия.

Удалённую или дистанционную работу можно описать как «использование информационно-коммуникационных технологий (ИКТ), таких как смартфоны, планшеты, ноутбуки и стационарные компьютеры, для выполнения работы за пределами помещения работодателя» [4]. Иначе говоря, это работа, которая выполняется при помощи ИКТ отдельно от работодателя.

До событий пандемии лишь незначительная часть работников в мире периодически существовала в режиме «удалёнки». По данным «Eurofound and ILO» от 2017 года до резкого ухудшения эпидемиологической обстановки «в Европейском союзе регулярная или эпизодическая дистанционная работа (надомная и мобильная вместе взятых) составляла 30 и более процентов в Дании, Нидерландах и Швеции до

10% и менее в Чешской Республике, Греции, Италии и Польше. По данным разных исследований, до 20% рабочей силы в Соединенных Штатах регулярно или периодически работали дома или в другом альтернативном месте, в Японии – 16%, а в Аргентине - всего 1,6%» [4].

Опираясь на данные экспертно-аналитического центра «InfoWatch», можно оценить риск утечек информации в мировом масштабе и сопоставить аналитические данные с фактом роста популярности удалённой работы [1]. Например, в 2020 году было зафиксировано на 4,5% меньше утечек данных из организаций в мире, чем в 2019 году, но на 5,8% больше, чем в 2018 году, но по итогам 2022 года выросло в 3,5 раза (См. Табл. 1).

Таблица 1 – Утечки данных из коммерческих, некоммерческих (государственных, муниципальных) организаций в странах мира, шт. [1]

Количество утечек по годам	**2022**	**2021**	**2020**	**2019**	**2018**
	6856	1729	2406	2639	2436

Если рассматривать период с 2018 по 2020 гг. можно заметить, что тенденция роста доли утечек умышленного характера (как внешних, так и внутренних) сохраняется, хотя доля общих утечек внутреннего характера постепенно снижалась. В этот же период общая доля умышленных утечек персональных данных выросла с 60,2% до 72,5%, чему в принципе мог способствовать факт смены режима работы. Доля утечек платежной информации всех видов в 2020 по сравнению с 2019 годом сократилась в 2 раза, а в сравнении с 2018 – более чем 3 раза, что свидетельствует о повышении внимания организаций к информационной безопасности. 55,9% утечек были инспирированы внешними нарушителями, внутренние нарушители осуществили еще 44,1% утечек.

Сложностью перехода сотрудников из одного режима в другой способствовала тому, что 35,4% утечек стали результатом умышленного или не умышленного воздействия непривилегированных сотрудников. Скомпрометированными за 2020 год оказались более 11 млрд. записей персональных данных и платежной информации. 84 утечки были учтены в 2020 году, результатом каждой из них явилась «потеря» более 10 млн записей. На столь значительные утечки пришлось 95,7% всех записей, у которых была нарушена конфиденциальность. [1]

В общем массиве утечек с числом скомпрометированных записей менее 1 млн. каждая, в 2020 году на каждую утечку в среднем пришлось 28,1 тыс. записей, против 19,9 тыс. записей в среднем на утечку в 2019 году. Увеличение масштабности хакерских атак может быть связано со сложностью перехода на «удалёнку» и недостаточной подготовкой работников к этому процессу. Около 2,8 млн. записей в 2020 году пришлось на утечку из внешнего контура, 6,8 млн. записей это утечки внутри защищаемого периметра.

При всём этом более 79% утечек в 2020 году происходило через сеть Интернет. Это говорит о том, что резкий рост востребованности дистанционной работы пошёл на руку злоумышленникам, работающим через всемирную сеть. Доля утечек при помощи электронной почты и традиционных документов на бумажном носителе на протяжение 2018–2020 гг. постепенно падала.

В связи с ослаблением контроля за обращением данных при удалённой работе вследствие ковидных ограничений наблюдался рост количества умышленных утечек персональных данных и сведений коммерческой тайны. Данную тенденцию можно увидеть, проанализировав период с 2018 по 2020 годы.

Рассматривая данные 2021 года, можно предположить, что общая доля утечек снизилась по сравнению с предыдущими годами, так как система удалённой работы стала более налажена. Но это не отменяет факта наличия в этот год довольно крупных информационных утечек [2].

Одной из таковых стала самая крупная зафиксированная утечка медицинской информации в августе 2021 года. Около 886 млн. записей пациентов было обнаружено на облачном сервере компании «Deep 6 AI», которая разрабатывает для сферы здравоохранения системы на основе искусственного интеллекта.

Утечки внутреннего характера обычно характеризуются относительно небольшими базами данных или отдельными записями, так как украсть большой массив данных незаметно довольно сложно. Но в 2021 году в «Alibaba Group» произошла крупная утечка информации.

Один из разработчиков на протяжении восьми месяцев копировал персональные данные пользователей платформы электронной коммерции «Taobao». Всего скомпрометирована конфиденциальная информация 1,1 млрд. человек. Злоумышленника интересовали такие данные, как ID, номера телефонов и отзывы.

Еще одна крупная утечка 2021 года произошла в бразильском маркетплейсе «Hariexpress». Из-за некорректных настроек облачного сервера Elasticsearch были скомпрометированы более 1,75 млрд. записей персональных данных объемом порядка 600 ГБ. В частности, утекли полные имена, электронные адреса, номера бразильской системы зарегистрированных юрлиц, номера телефонов, домашние адреса, зашифрованные пароли.

Экспертно-аналитический центр «InfoWatch» зарегистрировал 404 случая утечки данных в Российской Федерации. Это были данные из коммерческих, государственных и муниципальных организаций. В 2019 году таких утечек было на 2,2 % меньше, а именно 395 [3].

В России утечка информации, опубликованной на языках, используемых в странах с высоким уровнем цифровизации, за 2020 год составила 16,9 % от мирового распределения. Только записей персональных данных и платежной информации утекло за год в количестве более 100 млн. При этом зафиксировано 15 крупных утечек, скомпрометировано при каждой из которых было от 1 млн. записей. Причем объем утечек данных в России в 2020 году в среднем составил 28,1 тыс. записей, а в 2019 году средний объем утечки составлял 19,9 тыс. записей. Очень показательно, что 79% нарушения конфиденциальности данных были из-за внутренних нарушителей, и только 21 % из-за внешних. Результатом умышленных действий стали почти 80 % всех утечек. Это опровергает предположение, о том, что утечки могли быть связаны с ошибками некомпетентных сотрудников, и банальной неподготовленностью сотрудников и руководителей к экстренному переходу на дистанционный режим работы. Однако и доля утечек умышленного характера по вине «своих нарушителей» выросла очень значительно с 38,7% в 2018 г. до 79,3% в 2020 г. 7 утечек в общем распределении в России произошла по вине пользователей с привилегированными правами, а именно руководителями и системными администраторами. Через мессенджеры, т. е. каналы мгновенных сообщений, происходит почти 20% утечек.

Отсюда можно сделать вывод, что, несмотря на довольно спорные показатели утечек по миру и то, что в России одним из основных направлений защиты информации в государственных информационных и телекоммуникационных системах выступает предотвращение утечек данных, в том числе по техническим каналам, переход на дистанционный формат работ значительно увеличил риск компрометации разного рода информации.

«Основными организационно-техническими мероприятиями по защите информации в общегосударственных информационных и телекоммуникационных системах в данной сфере в России является: сертификация средств защиты информации и контроля эффективности их использования, а также защищенности информации от утечки по техническим каналам систем и средств информатизации и связи» [6].

Комплекс мероприятий, направленных на защиту информации от не санкционированного к ней доступа по любым каналам и предполагающий

нейтрализацию воздействий на данные, в том числе уничтожение, искажение, блокирование доступа к информации, является технической защитой информации [5].

Для защиты от возможных утечек информации, как во время удалённой работы, так и при обычном режиме, можно рекомендовать некоторые методы защиты информации:

1. Готовиться к ликвидации угроз информационной безопасности и ее эффективности.

2. Распределение информации разнородной ценности в различных зонах, контролируемых соответствующим уровнем безопасности.

3. Установление приоритета для наиболее важной информации в предотвращении угроз утечки.

4. Повышение эффективности всей системы безопасности, имеющей многокомпонентный характер.

5. Создание в интегрированных системах централизованных служб безопасности.

6. Регулярное проведение аудита системы информационной безопасности предприятия.

При организации удалённой работы особое значение приобретают организационные меры по обеспечению информационной безопасности. Они должны лежать в основе всех мероприятий по построению системы защиты информации. От качества организационная работа зависит эффективность системы защиты информации в целом.

Следующим уровнем системы безопасности является аппаратно-программные меры. В основе этого уровня лежат электронные устройства в совокупности со специальными программами, выполняющими функции защиты, например, аутентификацию и идентификацию пользователей, запись всех событий в системе, шифрование данных и т.п.

Для аутентификации и идентификации пользователей могут применяться не только программные, но и аппаратные средства: ключи, магнитные карты, дискеты и т.д.

Состояние системы защиты информации предприятия при любых условиях работы сотрудников определяется принятием его топ-менеджментом своевременных и взвешенных решений на основании текущей ситуации с защитой информации по внутреннему и внешнему контуру, а также по результатам аудита системы информационной безопасности с учетом действующих законодательных актов.

Перечень использованной литературы и источников:

1. InfoWatch. Исследование утечек информации ограниченного доступа в 2020 году – 16.07.2021. – URL: https://www.infowatch.ru/analytics/analitika/issledovanie-utechek-informatsiiogranichennogo-dostupa-v-2020-godu (дата обращения 21.11.2023).

2. InfoWatch, Персональные данные: пять главных утечек года – 20.08.2023. – URL: https://www.infowatch.ru/analytics/daydzhesty-i-obzory/personalnye-dannye-pyat-glavnykhutechek-goda (дата обращения 21.08.2023).

3. InfoWatch, Россия: утечки информации ограниченного доступа, 2020 год – 06.07.2021. URL: https://www.infowatch.ru/analytics/analitika/rossiya-utechki-informatsii-ogranichennogo-dostupa-2020-god (дата обращения 21.11.2023).

4. International Labour Organization. Дистанционная работа по время и после пандемии COVID-19. Практическое руководство. – Москва, МОТ, 2020. – URL: https://www.ilo.org/wcmsp5/groups/public/-europe/---ro-geneva/---sromoscow/documents/publication/wcms_754535.pdf (дата обращения 21.12.2023)

5. Гатауллин Д.Ш., Девяткин Д.Е. Технические каналы утечки информации и способы защиты от них // Экономика и социум. – 2018. - № 4 (47). – URL: https://readera.org/tehnicheskiekanaly-utechki-informacii-i-sposoby-zashhity-ot-nih-140236453 (дата обращения 21.12.2023).

6. Российская Федерация. Президент Российской Федерации. Об утверждении Доктрины информационной безопасности Российской Федерации: Указ Президента РФ от 05.12.2016 № 646 // СПС «КонсультантПлюс».

4.4. ИСПОЛЬЗОВАНИЕ КОРПОРАТИВНЫХ ИНФОРМАЦИОННЫХ СИСТЕМ В КОНТЕКСТЕ УПРАВЛЕНИЯ ОТРАСЛЕВОЙ ИНФОРМАЦИОННОЙ БЕЗОПАСНОСТЬЮ НА ПРЕДПРИЯТИЯХ ИНДУСТРИИ ТУРИЗМА И ГОСТЕПРИИМСТВА

В статье рассмотрены аспекты использования корпоративных информационных систем (КИС)) в контексте управления отраслевой информационной безопасностью (ИБ) на предприятиях индустрии туризма и гостеприимства.
Ключевые слова: автоматизация, информационная безопасность (ИБ), информационные технологии (ИТ), информация, корпоративные информационные системы (КИС), предприятия индустрии туризма и гостеприимства.

THE USE OF CORPORATE INFORMATION SYSTEMS IN THE CONTEXT OF INDUSTRY INFORMATION SECURITY MANAGEMENT AT ENTERPRISES OF THE TOURISM AND HOSPITALITY INDUSTRY

The article discusses aspects of the use of corporate information systems in the context of industry information security management at enterprises of the tourism and hospitality industry.
Keywords: automation, information security (IS), information technology (IT), information, corporate information systems (CIS), tourism and hospitality industry enterprises.

Современные информационные технологии (ИТ) приобретают большое значение в управленческом процессе. Все чаще специалисты оперируют понятиями локальная сеть, интернет-маркетинг, корпоративные информационные системы и т.д. Использование компьютеризированных средств обработки и передачи информации позволяет повысить скорость и качество принятия решений, обеспечить новые конкурентные преимущества, сократить транзакционные издержки, обеспечит информационную безопасность и пр. [33, с. 5].

Корпоративная информационная система (КИС) – важнейшая составляющая современной информационной инфраструктуры сложной организации, так как потребность в информационной системе характерна только для организаций, обладающих высокой мерой сложности – значительным количеством подразделений и многочисленными направлениями деятельности.

КИС – это комплекс программно-аппаратных средств, обеспечивающих бизнес-процессы организации. Иногда в определение корпоративной информационной системы не включаются аппаратные средства, так как большинство КИС могут быть реализованы на уже имеющемся в организации компьютерном оборудовании при его соответствии аппаратным требованиям КИС.

Использование КИС на предприятиях индустрии туризма и гостеприимства позволит повысить качество информации, экономичность документооборота и удобство для работников предприятий.

По мнению специалистов, для единого пространства хранения и обработки корпоративных документов наиболее подходит система «Корпоративный документооборот». Среди конкурентных преимуществ СЭД «Корпоративный документооборот» выделяются следующие основные моменты:

- система содержит в себе визуальный редактор бизнес-процессов. Таким образом, существует возможность разрабатывать сложные (в том числе вложенные) бизнес-процессы без программирования и изменения структуры программы, что облегчает установку обновлений и сокращает траты на сопровождение программы;

- в основную поставку систему включена подсистема управления ключевыми показателями эффективности (KPI). Она позволяет создать интегрированную с бизнес-процессами и документооборотом систему оценки эффективности работы предприятия и его сотрудников;

- в основную поставку также включена подсистема технической поддержки (на основе стандартов ITIL) с корпоративной базой знаний, что позволяет без особых затрат организовать на предприятии собственную службу технической поддержки, что упорядочит работу и снизит нагрузку на отдел ИТ [1. с.128].

Ведение информационного учета и анализа предприятии сферы туризма и гостеприимства связано с большим количеством нюансов. В ходе исследования корпоративных бизнес-процессов, было выявлено, что для дальнейшего успешного ведения внутреннего документооборота необходима его оптимизация.

В контексте индустрии гостеприимства (сектор питания) широко используется программа «Storehouse», которая является дополнением к системе R-keeper (POS-система для автоматизации организаций общественного питания: кафе и ресторанов, баров и точек быстрого питания), которая позволяет оптимизировать автоматизацию управления объектом общественного питания, существенно упрощает ведение учета. В то время как «R-keeper» отвечает за автоматизацию работы зала, кассы и кухни заведения, система «Storehouse» обеспечивает успешное ведение складского учета. Она контролирует движение товара с момента его поступления в организацию и до времени реализации. Приложение предоставляет информацию обо всех проходящих с товаром операций, связанных с приходом, расходом, перемещением, возвратом, списанием, комплектацией и декомплектацией, обеспечивая ее сохранность и безопасность. Возможности системы по работе с документами:

- система дает возможность создавать и обрабатывать такие документы, как: приходные накладные, расходные накладные, документы внутренних перемещений, сличительные ведомости, документы возврата товара поставщику, документы списания испорченных продуктов, комплектации, счета-фактуры, документы о расходе блюд;

- в зависимости от статуса документов (активный/неактивный) они могут участвовать или не участвовать в пересчете себестоимости, при этом статус документа задается пользователем и легко изменяется;

- при сохранении активных документов по каждому из продуктов показывается остаток после операции;

- продукты в документах могут быть заданы в любых, определенных для этих продуктов, единицах измерения;

- любые документы могут копироваться в документы других типов;

- данные из ведомости остатков могут копироваться в любой из типов документов;

- при проведении инвентаризации можно использовать весы для определения остатков товаров с учетом массы тары (в том числе и спиртных напитков);

- при проведении инвентаризации система информирует о выявленных излишках или недостаче;

- при заведении документов имеется возможность использовать сканер для чтения штрих-кодов;

- предлагаемые выходные формы документов унифицированы и соответствуют государственным стандартам.

Система «StoreHouse» позволяет сформировать следующие виды отчетов: ведомость остатков, оборотная ведомость товаров, движение товара, обороты по документам, последний приход/расход, товарный отчет, расчеты с поставщиками/получателями, анализ поставщиков, движение продуктов в производстве, заявка на закупку товара, акты реализации, анализ реализации, сводный анализ реализации, продажи блюда, продажи по дням, продажи по категориям, относительные суммы по продажам, расход продуктов по нормам рецептур, список блюд, список рецептов, калькуляции по дням, калькуляции по продажам, список калькуляций по продажам [2, с. 28].

Общим критерием оценки целесообразности автоматизации решения экономических задач является достигаемый экономический эффект от внедрения программного средства, именно снижение стоимостных затрат при обработке данных, оптимизация деятельности при работе с документами, и за счет этого достижение экономии на материалах или затратах на обработку, снижение трудовых затрат, и в связи с этим оптимизация кадрового состава организации за счет изменения количества работников и оптимизации их труда. Все полученные изменения необходимо оценить с точки зрения экономии рабочего времени и фонда заработной платы, получения снижения затрат на разработку документов или производственных, или логистических процессов, а также информационной безопасности.

Обычно для оценки экономической эффективности автоматизированного проекта сравнивают изменение трудовых и стоимостных затрат на обработку информации в сравнении базового варианта, т.е. того который был до внедрения информационных технологий (это может быть ручная обработка документов) и новый предлагаемый вариант автоматизации.

К трудовым затратам относятся следующие показатели, которые характеризуют трудоемкость работы [5, с. 28]:

1) абсолютное изменение затрат по труду (ΔT) (час/год):

$$\Delta T = T_0 - T_1$$

,

где Т0 – трудовые затраты по работе с документами без учета внедрения программных средств; Т1 – трудовые затраты на работу с документами по автоматизированному варианту, с использованием средств автоматизации;

2) коэффициент снижения трудовых затрат на выполняемые работы (КТ):

$$K_T = \left(\frac{\Delta T}{T_0}\right) \cdot 100$$

;

3) индекс уменьшения трудовых затрат на выполняемые работы (YT):

$$Y_T = \frac{T_0}{T_1}$$

.

К показателям изменения стоимости относятся:

1) абсолютное изменение затрат на обработку информации (ΔC) [руб./год.]:

$$\Delta C = C_0 - C_1$$

,

где С0 – стоимостные затраты на работу с документами без использования средств автоматизации (руб./год); С1 – стоимостные затраты на работу с документами с использованием систем автоматизации (руб./год);

2) коэффициент относительного снижения стоимостных затрат (Кс):

$$K_C = \left(\frac{\Delta C}{C_0}\right) \cdot 100$$

;

3) индекс производительности труда (Yc):

$$Y_C = \frac{C_0}{C_1}$$

Коэффициенты Кс и Yc характеризуют изменение производительности труда за счет внедрения информационных систем и средств, позволяющих экономить время на обработку данных.

При оценке эффективности используются различные показатели, которые характеризуют изменение поведения проекта в частных значениях, или обобщенные.

Годовой экономический эффект использования проекта автоматизации (Э) определяется как разность между годовой экономией и нормативной прибылью (руб./год):

$$Э = \Delta C - К_П \cdot Е_Н$$

,

где КП – разовые затраты, тыс. руб.; ЕН – нормативный коэффициент эффективности капитальных вложений.

К разовым затратам относятся затраты на разработку и выполнение этапов проектирования комплекса задач, а также затраты на программную реализацию и внедрение полученного программного продукта в информационное пространство организации заказчика. Произведение разовых затрат и нормативного коэффициента эффективности капитальных вложений в данном случае следует рассматривать как нормативную прибыль (в руб.), которая должна быть получена от внедрения системы. Значение ЕН принимается равным 0,15 для всех отраслей народного хозяйства.

Разовые затраты (КП) рассчитываются по формуле: КП = СПРОЕКТ + СПРОГР + СОТЛ + СМАШ, где СПРОЕКТ – затраты на выполнение этапов проектирования программного продукта (руб./год); СПРОГР – затраты реализацию проекта (рублей/год); СОТЛ – затраты на тестирование, внедрение и настройку (руб./год); СМАШ – затраты на машинное время (руб./год).

Срок окупаемости (ТОК) (руб./год) представляет собой отношение капитальных затрат на внедрение средств автоматизации к годовой экономии:

$$Т_{ок} = \frac{К_П}{\Delta C}$$

.

Расчетный коэффициент экономической эффективности капитальных затрат (ЕР) представляет собой отношение годовой экономии (годового прироста прибыли) к капитальным затратам на внедрение средств автоматизации:

$$Е_р = \frac{\Delta C}{К_П} = \frac{1}{Т_{ок}}$$

.

При ручной обработке рассчитываются следующие итоговые показатели:

1) трудоемкость обработки одного i-го документа (Toi) (в час) с учетом использования клавишных вычислительных машин:

$$Т_{oi} = \frac{Q_{зi}}{Н_з} + \frac{Q_{сi}}{Н_с} + \frac{Q_{уi}}{Н_у} + \frac{Q_д}{Н_д}$$

,

где Qзi – объем символов записи по i-ому документу; Qci – количество операций сложения по i-ому документу; Qyi – количество операций умножения по i-ому документу; QДi – количество операций деления по i-ому документу; Нз; Нс; Ну; Нд – среднечасовая выработка для соответствующей операции.

Нормативы для расчета показателей выполнения операций представлены в таблице 1 [6, с.104].

Таблица 1 – Нормативы для расчета трудоемкости ручных операций

Наименование операции	Единица измерения	Условное обозначение выработки	Среднечасовая выработка
Запись	Знак	$Н_З$	5600
Сложение/вычисление	Действие	$Н_С$	600
Умножение	Действие	$Н_У$	210
Деление	Действие	$Н_Д$	170

2) трудовые затраты при ручной обработке (То) (в час):

$$Т_о = \sum_{i=1}^{N} Т_{oi} \cdot n_i$$

,

где ni – количество документов, обрабатываемых вручную и с использованием калькулятора; N – количество видов (наименований) документов;

3) стоимостные затраты при ручной обработке (С0) (руб./год):

$$С_0 = р \cdot Т_0 \cdot (1 + К_g)$$

,

где р – часовая ставка заработной платы работника в рублях; Kg – коэффициент, учитывающий дополнительную заработную плату (0,53–0,85).

При обработке с помощью вычислительных средств рассчитываются следующие показатели:

1) трудоемкость операции (в час):

$T_{ij} = \frac{Q_j}{H_j}$ (кроме ЭВМ), $T_{iЭВМ} = t_m$, где Tij; TiЭВМ – трудоемкость i-ой операции и при обработке на ЭВМ соответственно; Qj – объем работы на j-ой операции; Hj – среднечасовая норма выработки на j-ой операции; tM – машинное время решения задачи на ЭВМ;

2. Заработная плата пользователей системы (руб./год):

$C_{ЗПj} = P_j \cdot T_{ij}$;

3) прочие расходы на выполнение работ по обработке документов по продажам или деятельности организаций (руб./год):

$C_{gj} = C_{зj} \cdot K_{gj}$;

4) амортизационные отчисления на оборудование, которое используется в процессе работы со средствами автоматизации (руб./год):

$C_{aj} = a_j \cdot T_{ij}$ (кроме ЭВМ);

5) расходы на текущую деятельность (руб./год):

$C_{ij} = C_{зпj} + C_{gj} + C_{aj}$ (кроме ЭВМ), $C_{iЭВМ} = Ц_м \cdot t_M$,

где Czпj; Cgj; Caj – соответственно заработная плата оператора, прочие расходы и стоимость амортизации на j-ой операции; Pj – часовая тарифная ставка операции; Kgj – коэффициент, дополнительной заработной платы (0,6 – 0,8); aj – сумма амортизации в часах; Cj; CiЭВМ – общие стоимостные затраты на j-ой операции и при обработке на ЭВМ соответственно; ЦМ – стоимость машинного часа ЭВМ;

6) трудовые затраты при машинной обработке (Ti) (час/год):

$T_i = \sum_{j=1}^{M} T_{ij}$, где M – количество операций [в год];

7) стоимостные затраты при машинной обработке (Ci) (руб./год):

$C_i = \sum_{j=1}^{M} C_{ij}$

В прикладном аспекте мы будем ориентироваться на данные, предоставленные одним из объектов общественного питания города Красноярска. Важно помнить, что большинство показателей являются средними величинами поскольку рассчитать каждый документ при оценке документопотока невозможно. В таблице 2 представлены объемные характеристики потоков информации.

Таблица 2 – Объемные характеристики потоков информации

Документ	**Количество строк в одном документе**	**Количество документов в месяц**	**Годовой объем информации в величинах:**		
			Документах	**Документостроках**	**Символах**
Меню	349	13	156	54444	2376816
Блюда	31	15	180	5580	138420
Закупка продуктов	15	15	180	2700	37980
Рецептура блюд	25	48	576	14400	265536
Заказ блюд и товаров	25	47	564	14100	170328
Мероприятия	31	26	312	9672	244296
Итого по входным:			1968	100896	3233376
Отчет по выручке	31	15	180	5580	139 500

Отчет по общей выручке	502	1	12	6 024	259 032
Отчет по расходам на блюда	22	10	120	1 320	122 580
Итого по выходным:	-	-	312	34 932	1 068 588
ИТОГО:	**-**	**-**	**2280**	**135828**	**4301964**

Для расчета экономического эффекта произведен расчет объемных характеристик потоков информации с операциями по изменению данных в документах, которые представлены в таблице 3. Данные объемные характеристики показывают, с какими объемами данных приходится сталкиваться сотрудникам при выполнении своих должностных обязанностей.

Количество операций так же рассчитывается исходя из нормативных значений работы с информацией, поскольку каждый документ может, содержать разное количество информации.

Таблица 3 – Объемные характеристики потоков информации с операциями

Документ	**Количество документов в год**	**Объем информации в одном документе**			
		Символов записи	**Операций сложения/вычитания**	**Операций умножения**	**Операций деления**
Меню	864	200	0	0	0
Блюда	816	200	0	0	0
Закупки продуктов	1200	375	0	0	0
Рецептура блюд	600	225	0	0	0
Заказ блюд и товаров	300	700	0	0	0
Мероприятия	12	2200	0	0	0
Итого по выходным	3792	3920	0	0	0
Отчет по выручке	-	-	0	0	0
Отчет по общей выручке	864	1200	6	0	0
Отчет по расходам на блюда	840	380	6	0	0
Итого по выходным	1704	1580	0	0	0
ИТОГО:	**5496**	**5500**	**12**	**0**	**0**

Необходимо рассчитать T_0 – трудоемкость обработки данных по базовому (смешанному) варианту. В итоге суммарные трудозатраты на обработку входных и выходных документов составляют 1527 часов.

Далее необходимо рассчитать трудовые и стоимостные затраты по базовому (смешанному) варианту без автоматизации, а также по автоматизированному варианту. Результаты вычислений занесем в таблицы 4 и 5.

По этим таблицам видно, что трудоемкость Т0 обработки документов по базовому варианту без автоматизации составляет около 1948 часов в год, а стоимостные затраты C_0 на обработку документов – 588563,00 руб. в год. В то время как трудоемкость T_1 обработки документов по автоматизированному варианту с внедрением информационных систем составляет около 704 часа в год, а стоимостные затраты С1 на обработку документов – 202062,00 руб. в год.

Из таблиц 4 и 5 видны изменения трудовых и стоимостных затрат при использовании средств автоматизации объекта общественного питания по сравнению с

ручным документооборотом – экономия трудовых и стоимостных затрат предполагается более чем в 2 раза.

Таблица 4 – Расчет трудовых и стоимостных показателей по базовому (смешанному) варианту

Наименование операции	**Единицы**	**Оборудование**	**Объем контроля, часов в год**	**Норма выработки, ед. в час.**	**Трудоемкость T_0, часов в год**	**Часовая тарифная ставка, руб.**	**Часовая норма амортизации оборудования, руб.**	**Стоимость машинного часа, руб.**	**Затраты на з/п, руб./год**	**Накладные расходы, руб./год**	**Затраты на амортизацию, руб./год**	**Затраты на машинное время, руб./год**	**Общие затраты C_0, руб./год.**
Приме, визуальный контроль и регистрация	Док/строки		38 520	400	100	150,00	–	–	14 470,00	8 680,00	–	–	23 150,00
Обработка записей	Символы	ПЭВМ	–	–	1 530	150,00	5,00	60,00	229 350,00	137 610,00	7 630,00	91 590,00	466 180,00
Анализ результатов (выходные документы)	Док/строки		121 250	400	300	150,00	5,00	60,00	45 540,00	27 324,00	1 520,00	18 190,00	92 570,00
Печать и выдача выходных документов	Док/строки	ПЭВМ, принтер	121 250	5 600	20	150,00	7,00	60,00	3 250,00	1 950,00	150,00	1 300,00	6 660,00
Итого	–	–	–	–	**1 948**	–	–	–	–	–	–	–	**588 563,00**

Таблица 5 – Расчет трудовых и стоимостных показателей по автоматизированному варианту

Наименование операции	Наименование операции	Обработка	Верификация	Регистрация в ПЭВМ	Приме, визуальный контроль и регистрация	Анализ и выдача результатов	Печать и выдача выходных документов	Итого
Единицы	Символы	Операции	Символы	Символы	Док/строки	Док/строки	Док/строки	–
Оборудование	ПЭВМ	ПЭВМ	ПЭВМ	ПЭВМ	Нет	–	ПЭВМ, принтер	–
	1 157 640	5 788 000 000	1 157 640	1 157 640	38 520	121 250	121 250	–
Объем контроля, часов в год	7 000	3 600 000 000	10 000	7 000	400	400	5 600	–
Норма выработки, ед. в час.	170	2	120	170	100	300	20	**704**
Трудоемкость T_1, часов в год	150,00	150,00	150,00	150,00	150,00	150,00	150,00	–
Часовая тарифная ставка, руб.	5,00	5,00	5,00	5,00	–	5,00	7,00	–
Часовая норма амортизации оборудования, руб.	60,00	60,00	60,00	60,00	–	60,00	60,00	–
Стоимость машинного часа, руб.	24 840,00	17 390,00	240,00	24 840,00	14 470,00	45 540,00	3 250,00	–
Затраты на з/п, руб./год	14 900,00	10 430,00	150,00	14 900,00	8 680,00	27 320,00	1 950,00	–
Накладные расходы, руб./год	830,00	580,00	10,00	830,00	–	1 520,00	150,00	–
Затраты на амортизацию, руб./год	9 920,00	6 940,00	100,00	9 920,00	–	18 190,00	1 300,00	–
Затраты на машинное время, руб./год	50 490,00	35 350,00	490,00	50 490,00	23 150,00	92 570,00	6 660,00	**202 062,00**

Далее рассчитаем показатели эффективности от внедрения RBC.

При этом нужно учитывать погрешность, допущенную при расчете трудовых и стоимостных затрат. В расчетах рекомендуется брать погрешность в 15% от показателей трудовых и стоимостных затрат (См. Табл. 6) [2, с. 278].

Таблица 6 – Показатели эффективности от внедрения новой системы

	Затраты		Абсолютное изменение затрат	Коэффициент изменения затрат	Индекс затрат
	Базовый вариант	**Проектный вариант**			
Трудоемкость	**To (час)**	**Ti (час)**	**ΔT = To-Ti**	**Кт = ΔT/To·100%**	**Iт = To/Ti**
	1948	704	1244	63,86%	2,8
Стоимость	**Co(руб.)**	**C_1 (руб.)**	**$\Delta C = Co - C_1$**	**Кс = ΔC/Co·100%**	**Ic = Co/C_1**
	588563,00	202062,00	386501,00	65,66%	2,9

Для определения первоначальных капитальных вложений нужно рассчитать часовую заработную плату с учетом налогов и накладных расходов, а также количество часов, затрачиваемых на внедрение и настройку КИС.

Заработная плата программиста составляет 12000 руб. без учета ЕСН. Но нужна почасовая заработная плата: она составит 12000/(21 х 8) = 71,4 руб./час. Следовательно, с учетом накладных расходов (60%) – до 114,00 руб./час. Затраты на проектирование и внедрение проекта автоматизации объекта общественного питания представлены в таблице 7.

Таблица 7 – Расчет затрат на проектирование и внедрение проекта

Вид работ	Деятельность (час)	Стоимость (руб/час)	Затраты (руб)
Проектирование	24	114,00	2741,00
Программирование	96	114,00	10944,00
Отладка и внедрение	20	114,00	2280,00
Машинная реализация	116	114,00	13224,00
ИТОГО:			**29189,00**

Кроме того, необходимо учитывать и стоимость ПО «Storehouse» (рассчитанную на управляющего, бар, кухню, зал) – около 85000,00 руб., следовательно, в дальнейших расчетах будет использоваться сумма 114189,00 (29189,00 + 85000,00) руб.

Для расчета годового экономического эффекта от внедрения системы «Storehouse» нужно учитывать, что нормативный коэффициент эффективности капитальных вложений для всех отраслей народного хозяйства составляет 15%, следовательно:

$$Эмин = (386501,00 – 114189,00) \times 0,15 = 369372,65 \text{ руб.}$$

Теперь рассчитаем срок окупаемости капитальных затрат:

$$Ток1 = 114189,00 / 386501,00 = 0,29 (\sim 4 \text{ месяца})$$

Тогда расчетный коэффициент эффективности капитальных затрат составит:

$$Ep1 = 1/0,29 = 3,44.$$

Для того чтобы проект автоматизации считался эффективным необходимо, чтобы расчетный коэффициент эффективности капитальных затрат был больше 0,15. Как видно из расчетов, внедрение данной системы автоматизации объекта общественного питания является эффективным.

Таким образом, срок окупаемости проекта составляет примерно 4 месяца.

Поскольку затраты на внедрение средства автоматизации объекта общественного питания «Storehouse» единовременно меньше годового экономического эффекта, то можно сделать вывод о том, что система уже через 4 месяца после внедрения окупит себя, и будет приносить прибыль.

Отметим, что информация представляет собой один из основных, решающих факторов, который определяет развитие технологии и ресурсов в целом. В связи с этим, очень важно понимание не только взаимосвязи развития индустрии информации, компьютеризации, информационных технологий с процессом информатизации, но и определение уровня и степени влияния процесса информатизации на сферу управления и интеллектуальную деятельность человека [5, с.18].

В настоящее время для большинства коммерческих предприятий характерна слабая проработка вопроса использования упорядоченных систем ведения делопроизводства несмотря на то, что именно рациональное и четко организованное делопроизводство, определяющее документационное обеспечение управления организацией, информационную безопасность, могут существенно увеличить эффективность деятельности предприятия.

Перечень используемой литературы и источников:

1. Инструкции по работе с системой R-KEEPER VER. 7. [Электронный ресурс]. – URL: http://sg-cto.ru.
2. Белошапка М. Технология ресторанного обслуживания: Учебное пособие. / М. Белошапка. – Москва: Academia. – 2017. – 320 с.
3. Ковалев В.В. Введение в финансовый менеджмент / В.В. Ковалев. – Москва: Финансы и статистика. – 2016. –131 с.
4. Ковалев В.В. Введение в финансовый менеджмент / В.В. Ковалев. – Москва: Финансы и статистика. – 2012. – 768 с.
5. Круглова О.В. Информационные технологии в управлении: учеб. пособие / О.В. Круглова. – Дзержинск: Изд-во «Конкорд» – 2016. – 134 с.
6. Пестриков В.М. Инновационные технологии в автосервисе / В.М. Петсриков // Инновации. 2008. – №8(118). – С. 104-106.
7. Ситкин В.А. Автоматизация ресторана и кассовая техника: учеб. пособие / В.А. Ситкин, Н.В. Химич. – Москва: Сервис ККМ. – 2017. – 132 с.

СВЕДЕНИЯ О АВТОРАХ

АНЦИФЕРОВА Валентина Ивановна

- кандидат технических наук, доцент, доцент кафедры «Информационные технологии» ФГБОУ ВО «ВГЛУ имени Г.Ф. Морозова» ***(раздел 1.1)***

АВЕТИСЯН Татьяна Владимировна

*- старший преподаватель кафедры информационных систем и технологий АНОО ВО «ВИВТ» (****раздел 4.1)***

АНИСИМОВ Александр Леонидович

- доктор исторических наук, профессор, профессор кафедры ФГКОУ ВПО МВД России «ДФЮИ МВД России» ***(раздел 2.9)***

БАРСОВ Максим Георгиевич

- студент (бакалавриат) 3 курса ФГБОУ ВО «МТУСИ» ***(раздел 2.1)***

БУГАЕНКО Андрей Валерьевич

- кандидат педагогических наук, доцент АНО «Университет 20.35» ***(раздел 2.2)***

ВАНДАНОВА Наталья Добаевна

- декан факультета телекоммуникаций БИИК (филиал) ФГБОУ ВО «СибГУТИ» ***(раздел 1.2)***

ВАНЮШИНА Анна Вячеславовна

- кандидат технических наук, доцент, доцент кафедры «Информационная безопасность» ФГБОУ ВО «МТУСИ» ***(раздел 2.3)***

ВОРОНОВ Александр Алексеевич

- доктор юридических наук, кандидат физико-математических наук, профессор АНОО ВО «ВИВТ»; ФКОУ ВО «ВИ ФСИН России» ***(раздел 4.2)***

ГВАРЛИАНИ Татьяна Евгеньевна

- профессор, доктор экономических наук, профессор кафедры экономики и финансов ФГАОУ ВО «СГУ» ***(раздел 3.1.)***

ДАНИЛОВ Роман Михайлович

- доцент, кандидат технических наук, заместитель директора по учебной и научной работе ХИИК (филиал) ФГБОУ ВО «СибГУТИ» ***(раздел 2.5)***

ДУШИНА Алина Сергеевна

- слушатель (очной формы обучения) 5 курса ФГКОУ ВПО МВД России «ВИ МВД России» ***(раздел 2.5)***

ЕЛЬКИНА Екатерина Дмитриевна

- студент (специалитет) 2 курса факультет кибербезопасности и управления ФГБОУ ВО «ПГУТИ» ***(раздел 1.3)***

ЕМЕЛЬЯНОВА Ольга Владимировна

- старший преподаватель кафедры ФГКОУ ВПО МВД России «МосУ МВД России имени В.Я. Кикотя» ***(раздел 1.4)***

ЖДАНОВА Татьяна Андреевна

- кандидат педагогических наук, доцент, доцент кафедры математики и информационных технологий ФГБОУ ВО «ТОГУ» ***(раздел 2.12)***

КАМАЕВА Алина Эльдаровна

- студент (специалитет) 2 курса факультет кибербезопасности и управления ФГБОУ ВО «ПГУТИ» ***(раздел 1.3)***

КИСЛИЦКИЙ Роман Русланович

- инженер Управления Росгвардии по Липецкой области ***(раздел 3.2.)***

КОБЕЛЕВ Константин Андреевич

- адъюнкт очной формы обучения ВУНЦ ВВС «ВВА имени профессора Н.Е. Жуковского и Ю.А. Гагарина» ***(раздел 1.5)***

КОВАЛЕНКО Татьяна Анатольевна

- кандидат технических наук, доцент, доцент кафедры «Информатики и вычислительной техники» ФГБОУ ВО «ПГУТИ» ***(раздел 1.3)***

КОВЫЛИНА Юлия Романовна

- студент (бакалавриат) 3 курса факультета «Информатика и вычислительная техника» ХИИК (филиал) ФГБОУ ВО «СибГУТИ» ***(раздел 1.8)***

КОРОВИНА Светлана Викторовна

- кандидат педагогических наук, доцент, доцент кафедры «Высшая математика» ФГБОУ ВО «ДВГУПС» ***(раздел 1.4)***

КРЕЙНДЕЛИН Виталий Борисович

- доктор технических наук, профессор, профессор кафедры «Информационная безопасность» ФГБОУ ВО «МТУСИ» ***(раздел 2.1)***

КРУНДЫШЕВ Василий Михайлович

- кандидат технических наук, доцент «Институт кибербезопасности и защиты информации» ФГАО ВО «СПбУ Петра Великого» ***(раздел 1.6)***

КУЛАГИНА Ирин Ивановна

- кандидат экономических наук, доцент, доцент кафедры информационных систем и математического моделирования ВолИУ – филиал ФГБОУ ВО «РАНХиГС»
(раздел 4.3)

ЛЬВОВИЧ Игорь Яковлевич

- доктор технических наук, профессор, АНОО ВО «ВИВТ» ***(раздел 4.1)***

ЛЬВОВИЧ Яков Евсеевич

- доктор технических наук, профессор, президент АНОО ВО «ВИВТ» ***(раздел 4.1)***

МАСЛОВ Григорий Федорович

- кандидат юридических наук, доцент, директор ХИИК (филиал) ФГБОУ ВО «СибГУТИ» ***(раздел 3.3)***

МЕЖУЕВ Дмитрий Александрович

- студент (магистратура) 2-го курса, ФГБОУ ВО «ВГУ» ***(раздел 1.5)***

МЕЖУЕВ Александр Михайлович

- доктор технических наук, доцент, начальник кафедры ВУНЦ ВВС «ВВА имени профессора Н.Е. Жуковского и Ю.А. Гагарина» ***(раздел 1.5)***

МОРОЗОВ Даниил Германович

- студент (специалитет) 2 курса факультет кибербезопасности и управления ФГБОУ ВО «ПГУТИ» ***(раздел 1.3)***

МОСКАЛЕНКО Филип Михайлович

- кандидат технических наук, научный сотрудник лаборатории интеллектуальных систем «Институт автоматики и процессов управления» ФГБУН «ДВО РАН» ***(раздел 1.7)***

НИКИТИНА Яна Юрьевна

*- студент (магистратура) курса «ДВИ (филиал) ФГБОУ ВО «ВУЮ (РПА Минюста России)» (****раздел 2.6)***

ОККЕЛЬ Светлана Алексеевна

- кандидат экономических наук, доцент, доцент кафедры «Менеджмента» ФГБОУ ВО «ДВГУПС» ***(раздел 2.7)***

ПОЛЯКОВ Родион Сергеевич

- студент (бакалавриат) 3 курса факультета «Информатика и вычислительная техника» ХИИК (филиал) ФГБОУ ВО «СибГУТИ» ***(раздел 1.8)***

ПРЕОБРАЖЕНСКИЙ Андрей Петрович

- доктор технических наук, профессор, профессор кафедры информационных систем и технологий АНОО ВО «ВИВТ» ***раздел 4.1)***

ПРЕОБРАЖЕНСКИЙ Юрий Петрович

- кандидат технических наук, доцент, доцент кафедры информационных систем и технологий АНОО ВО «ВИВТ» ***раздел 4.1)***

ПРОКОПЕКО Эдуард Феликсович

- старший преподаватель кафедры «Информационная безопасность» ХИИК (филиал) ФГБОУ ВО «СибГУТИ» ***(раздел 3.4)***

ПЫНЬКО Люсьена Евгеньевна

- кандидат экономических наук, доцент, доцент кафедры экономики и цифровых технологий «ДВИ – филиал ФГБОУ ВО «РАНХиГС» ***(раздел 2.6)***

РАХМАНИНА Наталья Викторовна

- кандидат юридических наук, старший преподаватель кафедры гражданско-правовых дисциплин ВолИУ – филиал ФГБОУ ВО «РАНХиГС» ***(раздел 2.8)***

РЕВУЦКАЯ Александра Алексеевна

- студент (бакалавриат) 3 курса факультета «Информатика и вычислительная техника» ХИИК (филиал) ФГБОУ ВО «СибГУТИ» ***(раздел 1.8)***

РЫБАК Александр Владимирович

- кандидат технических наук, доцент, профессор кафедры ФГКОУ ВПО МВД России «ДВЮИ МВД России» ***(раздел 2.4)***

САМОХИН Андрей Владимирович

- кандидат исторических наук, доцент, заместитель директора АНО «ЦИМО АТР» ***(раздел 2.9)***

СЕМЕНОВА Елена Владимировна

*- кандидат технических наук, доцент, доцент кафедры «Безопасность жизнедеятельности» АНОО ВО «ВИВТ» (****раздел 2.10)***

СИДОРОВ Сергей Александрович

*- доктор политических наук, доцент, доцент кафедры гражданско-правовых дисциплин ДВИ (филиал) ФГБОУ ВО «ВГУЮ (РПА Минюста России)» (****раздел 2.11)***

СТАСИТИС Дарья Витальевна

- студент (бакалавриат) 3 курса ФГБОУ ВО «ТОГУ» ***(раздел 2.12)***

СТЕПАНОВ Павел Владимирович

- кандидат химических наук, доцент, преподаватель кафедры ВУНЦ ВВС «ВВА имени профессор Н.Е. Жуковского и Ю.А. Гагарина» ***(раздел 1.9)***

СУХАНОВА Светлана Геннадьевна

– кандидат педагогических наук, доцент, доцент кафедры «Общепрофессиональных и гуманитарных дисциплин» ХИИК (филиал) ФГБОУ ВО «СибГУТИ» ***(раздел 3.5)***

ТАЛЫНЁВ Валерий Егорович

- доктор социологических наук, доцент, профессор кафедры ФГКОУ ВПО МВД России «ВИ МВД России» ***(раздел 2.5)***

ТРОПЫНИН Игорь Витальевич

- кандидат педагогических наук, доцент, доцент кафедры «Теоретические основы и менеджмент физической культуры и туризма» «Институт физической культуры, спорта и туризма» ФГАОУ ВО «СФУ» ***(раздел 4.4.)***

ТРОПЫНИНА Инесса Геннадьевна

- кандидат педагогических наук, доцент, доцент кафедры «Теоретические основы и менеджмент физической культуры и туризма» «Институт физической культуры, спорта и туризма» ФГАОУ ВО «СФУ» ***(раздел 4.4.)***

УСТИНОВ Игорь Юрьевич

- кандидат педагогических наук, доцент, заместитель начальника кафедры ВУНЦ ВВС «ВВА имени профессора Н.Е. Жуковского и Ю.А. Гагарина» ***(раздел 1.9)***

ШАХОВ Владислав Владиславович

– кандидат исторических наук, доцент, заместитель начальника кафедры ФГКОУ ВПО МВД России «БелЮИ МВД России имени И.Д. Путилина» ***(раздел 2.13)***

ШУЛЬЖЕНКО Николай Владимирович

- кандидат социологических наук, доцент, руководитель группы НИРиДО ХИИК (филиал) ФГБОУ ВО «СибГУТИ» ***(раздел 1.8)***

ЯРУЛИН Илдус Файзрахманович

- доктор политических наук, профессор, научный консультант «Институт социально-политических технологий и коммуникаций» ФГБОУ «ТОГУ»

(вводная статья)

ЯРЦЕВА Елена Павловна

- кандидат физико-математических наук, доцент, доцент кафедры математического моделирования, факультет математики и компьютерных наук имени профессора Н.И. Червякова ФГАОУ ВО «СКФУ» ***(раздел 1.10)***

Научное издание

ИНФОРМАЦИОННАЯ БЕЗОПАСНОСТЬ: ОБРАЗВАНИЕ. НАУКА. ОБЩЕСТВО.

(монография, посвящена Десятилетию науки и технологий в России и празднования 300-летия Российской академии наук)

Под общей редакцией:
Г.Ф. Маслова, Т.Е. Гварлиани, Р.М. Данилова, А.М. Межуева

Представленные работы изданы в авторской редакции

Подготовлено к печати Н.В. Шульженко
Дизайн обложки В.В. Громов

Подписано в печать 19.02.2024г.
Сдано в печать 20.02.2024г.
Заказ №
Бумага для множительных аппаратов.
Формат 60х84/16. Тираж 100 экз. Усл. печ. л. 10,6

Хабаровский институт инфокоммуникаций (филиал) ФГОБУ ВО
«Сибирский государственный университет коммуникаций и информатики»
ХИИК СибГУТИ
680000, г. Хабаровск, ул. Ленина 73.