Министерство науки и высшего образования Российской Федерации
НАЦИОНАЛЬНЫЙ ИССЛЕДОВАТЕЛЬСКИЙ
ТОМСКИЙ ГОСУДАРСТВЕННЫЙ УНИВЕРСИТЕТ (НИ ТГУ)
Институт экономики и менеджмента

ДОПУСТИТЬ К ЗАЩИТЕ В ГЭК
Руководитель ООП
канд. экон. наук, доцент
_____ В.В. Копилевич
«14» июня 2021 г.

ВЫПУСКНАЯ КВАЛИФИКАЦИОННАЯ РАБОТА СПЕЦИАЛИСТА
(ДИПЛОМНАЯ РАБОТА)

ИНФОРМАЦИОННАЯ БЕЗОПАСНОСТЬ: ОЦЕНКА СОСТОЯНИЯ, ИНСТРУМЕНТЫ УПРАВЛЕНИЯ И СПОСОБЫ ОБЕСПЕЧЕНИЯ (НА ПРИМЕРЕ ИНФОРМАЦИОННЫХ СИСТЕМ АДМИНИСТРАЦИИ ТОМСКОЙ ОБЛАСТИ)

по специальности 38.05.01 - Экономическая безопасность
специализация «Экономико-правовое обеспечение экономической безопасности»

Плахова Анастасия Андреевна

Руководитель ВКР
д-р. экон. наук, профессор
_____ Э. Г. Матюгина
подпись
«15» июня 2021 г.

Автор работы
студент группы № 27609/1
_____ А. А. Плахова
подпись
«15» июня 2021 г.

Томск 2021

Министерство науки и высшего образования Российской Федерации
НАЦИОНАЛЬНЫЙ ИССЛЕДОВАТЕЛЬСКИЙ
ТОМСКИЙ ГОСУДАРСТВЕННЫЙ УНИВЕРСИТЕТ (НИ ТГУ)
Институт экономики и менеджмента

УТВЕРЖДАЮ
Руководитель ООП
канд. экон. наук, доцент
_____ В.В. Копилевич
«__» декабря 2020 г.

ЗАДАНИЕ

по выполнению выпускной квалификационной работы специалиста (дипломной работы) обучающемуся Плаховой Анастасии Андреевне
(Ф.И.О. обучающегося)

по специальности 38.05.01 - Экономическая безопасность, специализация «Экономико-правовое обеспечение экономической безопасности»

1. Тема ВКР специалиста
Информационная безопасность: оценка состояния, инструменты управления и способы обеспечения (на примере информационных систем Администрации Томской области)

2. Срок сдачи обучающимся выполненной выпускной квалификационной работы специалиста:
в учебный офис «___»_____2021 г.
в ГЭК «___»_____2021 г.

3. Исходные данные к работе:
Объект исследования – информационная безопасность в аспекте выбора инструментов управления и способов ее обеспечения с учетом специфики организации функционирования территориальных органов управления.

Предмет исследования – совокупность параметров, характеризующих состояние информационной безопасности.

Цель исследования – оценка состояния информационной безопасности, а также исследование инструментов управления и возможных способов ее обеспечения на основе данных Администрации Томской области.

Задачи:
1) изучение теоретических основ информационной безопасности;
2) рассмотрение понятия информационной безопасности и определение ее связи с экономической безопасностью;
3) определение основных видов угроз;
4) исследование принципов и методов изучения информационной безопасности;
5) сравнение отечественного и зарубежного опыта применения средств защиты информации;
6) исследование информационных систем Администрации Томской области;
7) рассмотрение политики обработки защищаемой информации, не содержащей государственную тайну;
8) изучение модели угроз безопасности персональных данных;
9) оценка возможного ущерба Администрации при утечке персональных данных.

Методы исследования:
теоретические (классификация, синтез, анализ), практические (измерение, сравнение), специальные методы (интеллектуальный, исследовательский, прогнозный анализ данных), а также анализ полученных результатов путем статистической обработки, обобщение.

Организация или отрасль, по тематике которой выполняется работа:
Администрация Томской области

4. Краткое содержание работы:
1) исследование теоретических основ формирования и обеспечения информационной безопасности;
2) анализ инструментов управления и способов обеспечения информационной безопасности России и зарубежных стран;
3) рассмотрение информационных систем Администрации Томской области, оценка их текущего состояния и расчет возможных информационных угроз.

Руководитель ВКР

д. эк. наук, проф.		/ Э.Г. Матюгина
Должность	*подпись*	*инициалы, фамилия*

Задание принял к исполнению

студент		
	20.12.2020	Глахова А.Ф.
	дата / *подпись*	*фамилия студента*

АННОТАЦИЯ

Структура дипломной работы включает введение, 3 главы, 9 параграфов, заключение, список литературы и 2 приложения. Общий объем работы составил 84 страницы, в него вошли 7 рисунков, 7 таблиц, 2 формулы и 53 источника.

Цель исследования состоит в оценке состояния информационной безопасности, а также исследовании инструментов управления и возможных способов ее обеспечения на основе данных Администрации Томской области.

Объектом исследования выступает информационная безопасность в аспекте выбора инструментов управления и способов ее обеспечения с учетом специфики организации функционирования территориальных органов управления.

Предмет исследования состоит в совокупности параметров, характеризующих состояние информационной безопасности.

Результатом исследования является общая оценка состояния обеспечения информационной безопасности Российской Федерации, определенная как находящаяся на стадии развития, однако, уровень защищенности информации государственных органов является высоким и отвечающим международным требованиям. По результатам аналитической оценки уровня информационной безопасности систем Администрации Томской области был выявлен высокий уровень защиты электронных персональных данных.

Ключевые слова: информационная безопасность, информационная безопасность государственных органов, защита информации, Доктрина информационной безопасности, Администрация Томской области, Единая информационная система управления кадровым составом, цифровизация.

ОГЛАВЛЕНИЕ

ВВЕДЕНИЕ

Развитие информационных технологий экономического сектора стали неотъемлемой частью жизни современного общества, а поскольку информация является одним из самых ценных и важных ресурсов любого бизнес-процесса, информационная безопасность стала наиболее важным аспектом грамотного ведения бизнеса. Информационная безопасность включает комплекс мер, направленных на предотвращение и устранение несанкционированного доступа, обработки, искажения, форматирования, анализа, несогласованного обновления, исправления и уничтожения данных. Проще говоря, это набор мер, стандартов и технологий, необходимых для защиты конфиденциальных данных.

Проблема защиты информации от несанкционированного доступа и нежелательных воздействий существует давно, с развитием человеческого общества, появлением частной собственности, государственного строя, дальнейшим расширением человеческой деятельности информация приобретает все большее значение. Информация становится ценной, и ее владение позволит нынешним и потенциальным владельцам получать определенные выигрыши.

Переход на информатизированные системы коснулся и органов государственной власти. Большим шагом вперед в системе информационной безопасности стало электронное правительство. Электронное государственное управление не является дополнением к традиционному государственному управлению, а лишь определяет новый способ взаимодействия, основанный на активном использовании информационных и коммуникационных технологий для повышения эффективности предоставления государственных услуг.

Это обусловливает несомненную актуальность выбранной темы.

Вопросам изучения содержания и оценки состояния информационной безопасности посвящены труды отечественных и зарубежных ученых. Специфика защиты информации для органов госуправления рассмотрена в трудах таких авторов как Грунин О.А., Mueller J.P., Яблоков Н.П., Еськов А.В., Кирюшин И.И., Лободина А. С., Ермолаева В. В., Бирюков, А.А., Савченко О.А. и так далее.

Однако, необходимо отметить, что считать завершенными исследования в данной сфере вряд ли возможно в связи с непредсказуемостью и динамичностью изменения сред бизнеса, непрерывным совершенствованием информационных технологий, их глобальном охвате всех без исключения процессов жизнедеятельности общества и т.д.

Это обусловило следующую постановку цели дипломной работы – оценка состояния информационной безопасности, а также исследование инструментов управления и возможных способов ее обеспечения на основе данных Администрации Томской области.

Для достижения поставленной цели были использованы следующие задачи:

1) изучение теоретических основ информационной безопасности;

2) рассмотрение понятия информационной безопасности и определение ее связи с экономической безопасностью;

3) определение основных видов угроз;

4) исследование принципов и методов изучения информационной безопасности;

5) сравнение отечественного и зарубежного опыта применения средств защиты информации;

6) исследование информационных систем Администрации Томской области;

7) рассмотрение политики обработки защищаемой информации, не содержащей государственную тайну;

8) изучение модели угроз безопасности персональных данных;

9) оценка возможного ущерба Администрации при утечке персональных данных.

Объектом исследования является информационная безопасность в аспекте выбора инструментов управления и способов ее обеспечения с учетом специфики организации функционирования территориальных органов управления.

Предмет исследования – совокупность параметров, характеризующих состояние информационной безопасности.

Написание дипломного проекта включало следующие методы исследования: теоретические (классификация, синтез, анализ), практические (измерение, сравнение), специальные методы (интеллектуальный, исследовательский, прогнозный анализ данных), а также анализ полученных результатов путем статистической обработки, обобщение.

Информационная база исследования представлена трудами российских и зарубежных авторов, научными статьями, в которых нашли отражение анализ и оценка исследуемой проблемы, материалы открытых электронных ресурсов, а также подкреплена нормативно-правовыми актами (Федеральными законами, указами Президента, статьями Конституции).

Выпускная квалификационная работа содержит 83 страницы, 7 таблиц, 7 рисунков, 2 формулы, 2 приложения.

1. Теоретические основы формирования и обеспечения информационной безопасности

1.1 Понятие информационной безопасности, ее роль, основные компоненты

Ни одна система не может существовать без информационных потоков, нарушение или их недостаточность приводит к сбоям и потерям в эффективности и рентабельности, снижению динамики развития. Информация является важнейшей составляющей любой экономической системы.

Информационная сфера является системным фактором жизни общества и активно влияет на состояние политической, экономической, оборонной и других составляющих безопасности Российской Федерации. Национальная безопасность России существенно зависит от обеспечения безопасности информации, и эта зависимость будет усиливаться по мере технического прогресса.

В Доктрине информационной безопасности под термином информационная сфера понимается «совокупность информации, объектов информатизации, информационных систем, сайтов в информационно-телекоммуникационной сети «Интернет», сетей связи, информационных технологий, субъектов, деятельность которых связана с формированием и обработкой информации, развитием и использованием названных технологий, обеспечением информационной безопасности, а также совокупность механизмов регулирования соответствующих общественных отношений» [2, с. 69].

Поскольку существует вероятность потери целостности, доступности и конфиденциальности информации из-за наличия разносторонних угроз, она должна быть надлежащим образом защищена. Ежедневно каждый человек сталкивается с событиями, которые могут стать угрозами для информационной сферы, например:

1) присвоение чужого имущества;

2) кража собственности (информационного оборудования, комплектующих);

3) подделка данных, несанкционированная модификация;

4) нарушение прав частной собственности и конфиденциальности информации;

5) несанкционированный доступ или превышение прав санкционированного доступа к персональной информации владельца;

6) вымогательство или шантаж с использованием компьютеров;

7) несанкционированный доступ;

8) злонамеренное искажение или уничтожение данных;

9) нарушение авторского права или права интеллектуальной собственности и т. д.

Понятие информационной безопасности в Доктрине информационной безопасности РФ в широком смысле определено как состояние защищенности личности, общества и государства от внутренних и внешних, предумышленных и непредумышленных информационных угроз, которые гарантировано обеспечивают конституционные права человека и гражданина, безопасность, независимость и суверенность государства, территориальную целостность, высокий уровень жизни и устойчивое социально-экономическое развитие Российской Федерации [2, с. 69].

В узком смысле «информационная безопасность» - это состояние защищенности информации личности, общества и государства от случайных или целенаправленных воздействий естественного или искусственного характера с возможностью нанесения ими критического и непоправимого ущерба для субъектов информационных отношений.

Согласно Федеральному закону №149-ФЗ «Об информации, информационных технологиях и о защите информации» [3, с. 69] защита информации представляет собой принятие правовых, организационных и технических мер, направленных на:

1) реализацию защиты информации и от несанкционированного доступа, удаления, изменения, передачу, копирования, закрытия доступа и других возможных незаконных действий по отношению к информации;

2) ригоризм соблюдения защищенности информации закрытого доступа;

3) осуществление законного права на доступ и использование информации[1].

Основная задача информационной безопасности – минимизация и предотвращение рисков и угроз, а не ликвидация последствий. Именно принятие превентивных мер по обеспечению конфиденциальности, целостности и доступности информации является наиболее действенным подходом при создании системы информационной безопасности.

Объектами информационной безопасности является то, на что направлены действия негативного характера, которые наносят ущерб и действия, предотвращающие первые. Объекты, на которых сосредоточены негативные последствия в информационной сфере, являются:

1) все виды источников информации - информация, записанная на материальном носителе с реквизитами, позволяющими их идентифицировать;

2) система создания, распространения и использования информации (информационные системы и технологии, СМИ, библиотеки, архивы, кадры, нормативные документы и так далее).

[1] Об информации, информационных технологиях и о защите информации Федеральный закон от 27 июля 2006 г. N 149-ФЗ // КонсультантПлюс : справ. Правовая система. – Версия проф. – М., 2021. – Режим доступа : локальная сеть Науч. б-ки Том. гос. ун-та.

Под субъектами информационных отношений понимаются как владельцы, так и пользователи информации и поддерживающей инфраструктуры.

Для того, чтобы регулировать поведение субъектов информационной сферы существует ряд нормативно-правовых актов в целях реализации прав и обязанностей, которые направлены на обеспечение защиты объектов правоотношений. Здесь же законодатель вводит ограничения на информационные права и свободы в целях защиты интересов граждан, общества и государства. При формировании норм права, установления прав и обязанностей применяются методы гражданского, административного и конституционного права.

Для обеспечения безопасности как информационной сферы в целом, так её субъектов и объектов на законодательном уровне были приняты следующие нормативно-правовые акты[2]:

1. Федеральный закон от 27 июля 2006 г. № 149-ФЗ «Об информации, информационных технологиях и о защите информации»;

2. Федеральный закон от 27 июля 2006 г. № 152-ФЗ «О персональных данных»;

3. Федеральный закон от 06.04.2011 N 63-ФЗ «Об электронной подписи»;

4. Федеральный закон от 04 мая 2011 года № 99-ФЗ «О лицензировании отдельных видов деятельности»;

5. Постановление Правительства РФ от 21.03.2012 № 211 «Об утверждении перечня мер, направленных на обеспечение выполнения обязанностей, предусмотренных Федеральным законом "О персональных данных" и принятыми в соответствии с ним нормативными правовыми актами, операторами, являющимися государственными или муниципальными органами»;

6. Постановление Правительства от 1 ноября 2012 г. № 1119 «Об утверждении требований к защите персональных данных при их обработке в информационных системах персональных данных»;

7. Постановление Правительства от 06 июля 2015 г. № 676 «О требованиях к порядку создания, развития, ввода в эксплуатацию, эксплуатации и вывода из эксплуатации государственных информационных систем, и дальнейшего хранения содержащейся в их базах данных информации»;

8. Приказ Федеральной службы по техническому и экспортному контролю от 18 февраля 2013 г. № 21 «Об утверждении Состава и содержания организационных и

[2] Родичев Ю. А. Нормативная база и стандарты в области информационной безопасности [Текст] : учебное пособие для студентов, обучающихся по программам высшего образования укрупненной группы специальностей и направлений подготовки 10.00.00 «Информационной безопасность» / Ю. А. Родичев. - Санкт-Петербург [и др.] : Питер, 2017. - 254 с.

технических мер по обеспечению безопасности персональных данных при их обработке в информационных системах персональных данных»;

9. Приказ Федеральной службы по техническому и экспортному контролю от 11 февраля 2013 г. № 17 «Об утверждении Требований о защите информации, не составляющей государственную тайну, содержащейся в государственных информационных системах»;

10. Приказ Федерального агентства правительственной связи и информации при Президенте Российской Федерации от 13 июня 2001 г. № 152 «Об утверждении инструкции об организации и обеспечении безопасности хранения, обработки и передачи по каналам связи с использованием средств криптографической защиты информации с ограниченным доступом, не содержащей сведений, составляющих государственную тайну»;

11. Приказ Федеральной службы безопасности от 10 июля 2014 г. № 378 «Об утверждении состава и содержания организационных и технических мер по обеспечению безопасности персональных данных при их обработке в информационных системах персональных данных с использованием средств криптографической защиты информации, необходимых для выполнения установленных Правительством Российской Федерации требований к защите персональных данных для каждого из уровней защищенности»;

12. Методический документ, утвержденный руководством ФСТЭК России от 11 февраля 2014 г. «Методический документ. Меры защиты информации в государственных информационных системах».

Таким образом, сфера информационной безопасности имеет довольно обширную законодательную базу, которая несомненно развивается. Для этого учитываются все основные аспекты защиты информации, которые тоже, в свою очередь, не перестают совершенствоваться. Необходимо брать во внимание основополагающие категории информационной безопасности, известные еще с конца прошлого века и дорабатывать их, выискивая новые, менее затратные и более эффективные способы решения проблем.

Майкл Шрёдер и Джерри Зальцер в 1975 году в статье «Защита информации в компьютерных системах» стали первыми в мире, кто классифицировали сбои в получении, хранении и передаче информации, разделив их условно на 3 категории: неавторизованный отказ в доступе к информации, неавторизованное раскрытие информации и неавторизованное изменение информации. После этого данную классификацию усовершенствовали и стандартизировали вида, которым пользуются и по сей день в качестве основной:

1. Confidentiality с англ. — «конфиденциальность» — способность информации быть недосягаемой для третьих лиц или процессов, другими словами, быть доступной только для авторизированных и допущенных к системе лиц. Данный компонент является основным и первостепенным в информационной среде. Однако, перед фактическим использованием разработанных мер по ее реализации в Российской Федерации встает большое количество преград и проблем. Например, сведения о технических путях утраты информации являются закрытыми для посторонних, из-за чего множество легальных пользователей не имеют возможности оценить возможные риски. Также, существует целый ряд юридических и технических проблем, которые препятствуют самостоятельной криптографии в качестве основного инструмента для защиты персональных данных.

2. Integrity с англ. — «целостность» — способность информации сохранять правильность и целостность активов, то есть свойство информации, которая характеризует его устойчивость к случайному или преднамеренному уничтожению или нелегитимному преобразованию. Данный критерий условно делится на статическую и динамическую целостность (неизменность информационных объектов и связанную с правильным выполнением транзакций соответственно). Целостность информационной безопасности становится самым главным аспектом в случае, когда при помощи различной информации и на ее основе пользователи принимают решения о дальнейших действиях.

3. Availability с англ. — «доступность» — способность информации быть доступной и готовой к использованию по запросу пользователя, имеющего к ней доступ. Другими словами, это свойство информационной системы и всех ее данных и процессов предоставить доступ или произвести обмен информацией между зарегистрированными в общей сети пользователями. Основная цель информационной среды относительно ее пользователей – это предоставление любых легитимных информационных услуг, таких как передача, хранение, обработка запрашиваемой информации и так далее. Однако, если по какой-то причине предоставление запрашиваемых услуг невозможно, то это наносит ущерб лицам, запросившим информацию. Главная роль описываемого критерия особенно очевидна в таких типах систем управления как производственная, транспортная и т. д.

В совокупности эти три ключевых критерия информационной безопасности именуются триадой CIA.

В 1998 году член Ассоциации вычислительной техники, исследователь и консультант по информационной безопасности Донн Паркер дополнил триаду CIA еще тремя пунктами: подлинность, владение и контроль, польза. Усовершенствованную модель назвали Паркеровской гексадой (от hexad с англ. — «группа из шести предметов»), продемонстрированную в соответствии с таблицей 1.

Таблица 1 – Модель Паркеровской гексады[3]

Атрибут	Комментарий
Подлинность (аутентичность)	Под атрибутом «подлинность» понимается заявление об авторстве и точность его происхождения. К примеру, для того, чтобы удостовериться в подлинность подписи на бумажном или электронном носителе необходимо произвести либо сверку с теми документами, где она уже была проверена, либо произвести сверку обычного рукописного текста и оставленной подписью. В случае проверки электронной информации на авторство используются криптографические программы с открытым ключом.
Владение и контроль	Это такое состояние системы, при котором выстраивается связь между лицами, имеющими доступ к владению и использованию информации и устройством или физическим носителем информации. То есть, определение на санкционированность доступа к определенной информации.
Польза	Под атрибутом «польза» понимается состояние системы, которое обеспечивает удобство для пользователей и сотрудников в использовании системы. Так возникает меньшее желание действовать в обход системы.

Информационные технологии, которые используются отдельными пользователями в информационном пространстве, обязаны соответствовать требованиям и критериям внешней безопасности использования и внутренней безопасности их строения. Исходя из этого, по всему миру проводится множество исследований компьютерных устройств и

[3] Моделирование угроз информационной безопасности: различные подходы // Национальный открытый университет. – М., 2021. – С. 21-23.

операционных систем, а также на их основе дополняются и изменяются уже имеющиеся международные акты в сфере информационной безопасности.

Федеральные критерии информационной безопасности были разработаны как один из компонентов Американского Федерального стандарта по обработке информации (Federal Information Processing Standard), так как США является одной из передовых стран в сфере изучения, защиты и совершенствования информационных процессов. Главной целью их формирования было определение универсального и открытого для дальнейшего развития набора основных требований безопасности для современных информационных технологий. Стандарт определяет обоснованный и структурированный подход к разработке требований безопасности для продуктов информационных технологий с учетом областей их применения. Стандарт представляет собой обобщение основных принципов безопасности информационных технологий 1980х годов и обеспечивает преемственность по отношению к ним, чтобы поддерживать успех в области информационной безопасности.

Основополагающим понятием концепции информационной безопасности Федеральных критериев является понятия «профиль защиты». Профиль защиты – это нормативный документ, регламентирующий все объекты безопасности IT-продукта в виде требований к его конструкции, технологии разработки и квалификационного анализа. Один профиль безопасности обычно описывает несколько IT-продуктов, имеющих схожую структуру и назначение. Основное внимание в профиле защиты уделяется требованиям к составу средств защиты и качеству их реализации, а также их соразмерность ожидаемым угрозам безопасности[4].

В качестве примера используемых критериев информационной безопасности рассмотрим специальные критерии органа предварительного расследования[5]:

1) характеристика объекта диагностики;

1.1) наименование органа;

1.2) вид деятельности;

2) характеристика используемых информационных технологий;

2.1) вид и класс информационных технологий;

2.2) степень и уровень защиты, наличие обновлений;

3) характеристика средств информационной защиты (программные, аппаратные);

---

[4] Международные стандарты по оценке безопасности информационных технологий. Федеральные критерии безопасности информационных технологий // Справочник по информационной безопасности. – М., 2020. – 14 с.

[5] Яблоков Н. П. Криминалистическая методика расследования: история, современное состояние и проблемы: монография. М.: Норма, 2016. – 191 с.

4) характеристика сетевых соединений (наличие доступа к сети Интернет, вид сетевого соединения, степень информационной защищенности);

5) характеристика субъектов информационного обмена (надежность и уровень информационной защиты);

6) характеристика вида информации и режима доступа.

Исходя из данного классификатора, самая высокая возможная оценка по вышеперечисленным критериям равна 11, то есть это будет значить, что информация органа предварительного расследования находится в состоянии полной безопасности от несанкционированного доступа третьих лиц или вирусов. Государственные органы вправе сами устанавливать количество критериев и их обширность для того, чтобы в конечном итоге получить наиболее точную оценку. Для получения независимого и беспристрастного результата могут быть приглашены сторонние эксперты и аудиторы. По результатам данного исследования можем наблюдать, что уровень безопасности находится на уровне 45%. В дополнение, на рисунке 1 можно увидеть уровень соответствия информационной безопасности органа предварительного расследования по специальным компонентам классификатора безопасности информационных систем для полной характеристики исследуемого объекта, субъектов передачи информации, всех используемых средств блокирования несанкционированного доступа и соединений сети.

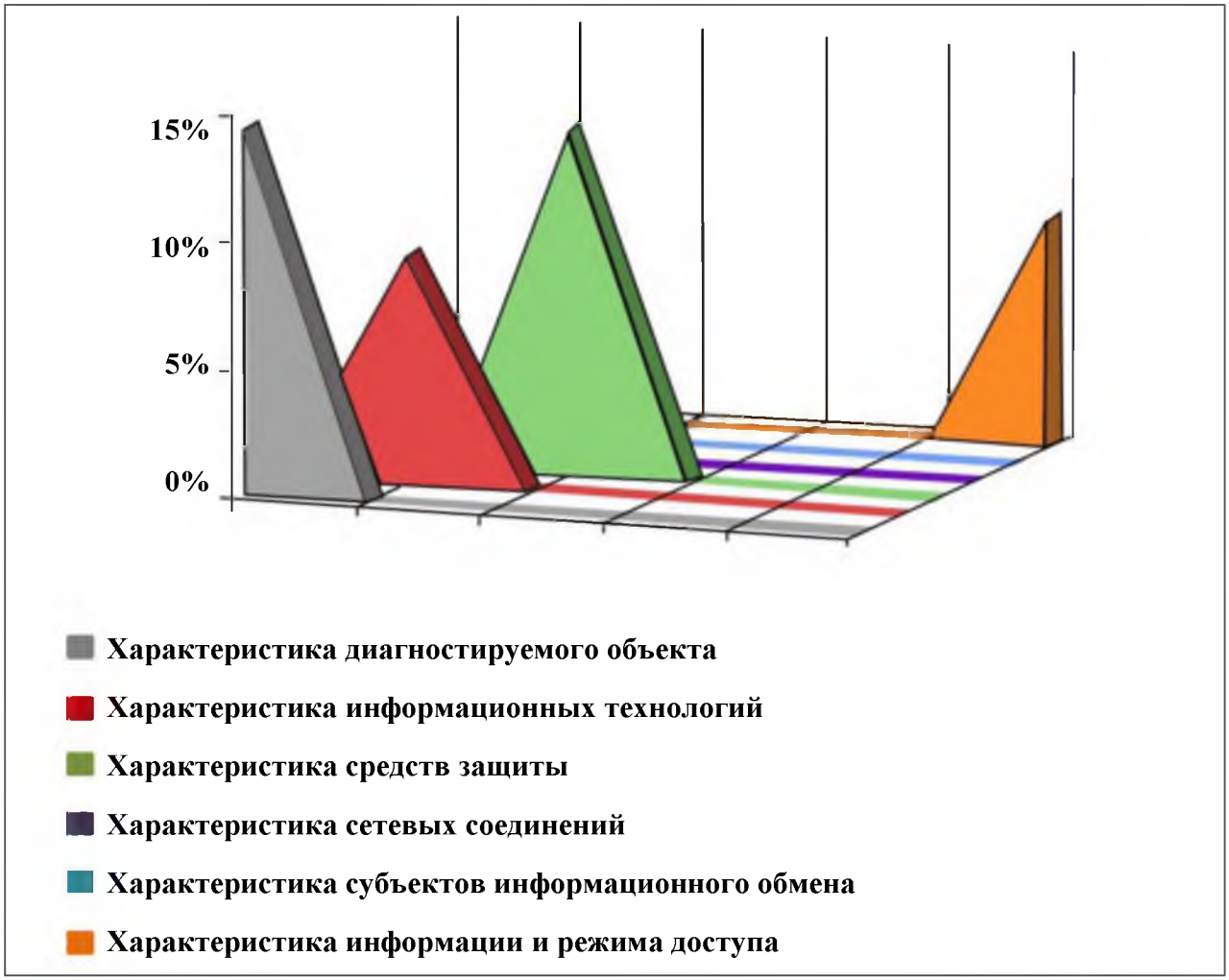

Рисунок 1 – Соответствие уровня защиты информационных технологий органа предварительного расследования специальным критериям его информационной безопасности[6]

Основываясь на полученных данных и оценке компонентов классификатора можно сделать вывод о том, что особые критерии информационной безопасности органов предварительного расследования в Российской Федерации – это одни из основных составляющих всей системы информационной безопасности и защиты технологий в структура правоохранительных органов. Учитывая, что особенные критерии рассматриваются в совокупности с общепринятыми анализ уровня безопасности, получается наиболее точным, так как общие критерии выходят на первый план и являются основополагающими при подсчете и изучении конкретного правоохранительного органа[7].

[6] Савченко О. А. Специальные критерии информационной безопасности органа предварительного расследования // Вопросы кибербезопасности. 2016. №2 (15). С. 4-6.

[7] Еськов А. В. Защита информационных систем с содержанием персональных данных, эксплуатируемых в ОВД / А. В. Еськов, И. И. Кирюшин // Проблемы правоохранительной деятельности. 2015. № 2. С. 76-79.

Организация экономического сотрудничества и развития в 1992 году создали модель информационной безопасности, в которую включили следующие принципы:

1) принцип ответственности;

2) принцип этики;

3) принцип демократии;

4) принцип осведомленности;

5) принцип противодействия;

6) принцип оценки рисков;

7) принцип пересмотра;

8) принцип разработки и внедрения информации;

9) принцип управления безопасности.

Однако, уже через четыре года после опубликования вышеназванных принципов Национальный институт стандартов и технологий (NIST), штаб-квартира которого базируется в городе Гейтерсберг, США, сформулировал принципы, которые гласят, что информационная безопасность является неотъемлемой составляющей рационального менеджмента, ограничивается социальными факторами, должна быть экономически эффективной, поддерживает миссию организации, должна периодически подвергаться пересмотру, требует всеобъемлющего и комплексного подхода, обязанности и ответственность за информационную безопасность должны быть четко сформулированы, а владельцы систем несут ответственность за безопасность не только внутри, но и за пределами своей организации[8].

В свою очередь, на основе этой модели NIST в 2004 году составил и утвердил 33 принципа инженерного проектирования систем информационной безопасности, которые неустанно развиваются, дополняются и поддерживаются в актуальном состоянии, включая практические руководства и рекомендации.

Несмотря на все доработки и совершенствования, отмеченные во всех вышеуказанных принципах и моделей информационной безопасности, первый вариант классической триады CIA 1975 года все равно остается основной и самой распространенной в международном профессиональном сообществе.

Безопасность информационных технологий и систем - одна из важнейших составляющих проблемы обеспечения экономической безопасности организации. Переход к новым формам управления в России в условиях дефицита и противоречивой правовой базы привел к ряду проблем с точки зрения защиты данных, информации, знаний и самих

[8] National Institute of Standards and Technology [Электронный ресурс] – URL: https://www.nist.gov/ (Дата обращения 10.05.2021).

ИКТ. Это своеобразие формирования рыночных отношений, отсутствие обоснованных концепций реформ и отставания в области применения современных информационных технологий в управлении и производстве. Обострение этих проблем высветило вопросы национальной, социальной и корпоративной безопасности, в том числе в информационной сфере.

Безопасность хозяйствующего субъекта может быть определена как «защита жизненно важных интересов государства или коммерческого предприятия от внутренних и внешних угроз, защита человеческого и интеллектуального потенциала, технологий, данных и информации, капитала и прибыли, обеспечиваемая системой правового, экономического, организационного, информационного, инженерного и социального характера»[9].

Для обеспечения целей экономической безопасности в секторе бизнеса и хозяйствующих субъектов необходимо обратить внимание на проблемные направления, такие как:

1) организация защиты финансовой, материальной и интеллектуальной собственности;

2) эффективное управления персоналом и ресурсами;

3) защиту информационных ресурсов организации.

В современных условиях успех бизнеса любой компании зависит в значительной степени от эффективности и мобильности компании, от своевременности и скорости принятия эффективных управленческих решений. А это невозможно без надежного и качественного информационного взаимодействия различных участников бизнес-процессов. Сегодня компании все чаще используют открытые каналы связи общедоступных сетей (Internet) и внутреннего информационного пространства компании (Intranet) в качестве среды для обмена информацией. Открытые Internet/Intranet каналы намного дешевле, чем выделенные линии. Тем не менее, общественные сети имеют существенный недостаток - открытость и доступность информационной среды. Компании не могут полностью контролировать передачу и прием данных по открытым каналам и в то же время гарантировать их целостность и конфиденциальность[10].

Глобализация мировых отношений сопровождается созданием эффективных средств и механизмов для информационного и экономического воздействия на

---

[9] Грунин О. А. Основы теории и практики экономической безопасности: Учеб. пособие / О. А. Грунин, С. О. Грунин; М-во образования Рос. Федерации. С.-Петерб. - СПб.: СПбГИЭУ, 2002, 90с.

[10] Безопасность информационных систем. Понятия экономической и информационной безопасности // Национальный открытый университет. – М., 2021. – С. 1-2.

конкурентов и партнеров в местном, региональном и глобальном уровнях. Целью таких воздействий, в основном, является изменение распределения произведенных реальных благ в пользу тех, кто разрабатывает, имеет и применяет соответствующие технологии. Сложившаяся ситуация требует повышенного внимания к защите государственных интересов от реальных и возможных угроз, обеспечения информационной и экономической безопасности.

Таким образом, роль информационной безопасности в наше время очень велика, так как в век компьютеризации большая часть информации хранится и передается при помощи информационных систем, а значит необходимо постоянно совершенствовать различные механизмы для поддержания безопасности информации на высоком уровне. Для того, чтобы понимать как действовать и какие меры предпринимать, специалисты в сфере компьютерной безопасности придерживаются общепризнанных критериев и принципов информационной безопасности.

1.2 Основные виды угроз. Методы обеспечения информационной безопасности

Российская компания InfoWatch, специализирующаяся на информационной безопасности в корпоративном секторе, то есть по защите организаций от утечек информации и атак извне, ежегодно публикует результаты исследований. В отчете 2020 года можно увидеть, что за первые 9 месяцев 2020 года в базу Экспертно-аналитического центра InfoWatch внесено 1773 случая утечки информации ограниченного доступа из коммерческих компаний, государственных организаций и органов власти во всем мире. В результате «утекло» 9,93 млрд записей персональных и платежных данных. По сравнению с аналогичным периодом 2019 г. в целом в мире число утечек снизилось на 7,4%, а число скомпрометированных записей – на 1,4%. За тот же период в России зафиксировано 302 утечки, что на 5,6% больше, чем за 9 месяцев 2019 г. Но количество «утекших» записей персональной и платёжной информации уменьшилось на 29,2% по сравнению с аналогичным периодом 2019 года (69,5 млн. записей)[11].

Снижение числа зарегистрированных утечек в мире главным образом можно объяснить влиянием пандемии COVID-19 на бизнес и государственный сектор: в результате ускоренной перестройки процессов и перевода значительной доли сотрудников

[11] Утечки информации ограниченного доступа: отчет за 9 месяцев 2020 года // Экспертно-аналитический центр InfoWatch. – М., 2020. – С. 9-13.

на удаленную работу контроль над информационными активами во многих компаниях был ослаблен, а значительная часть инцидентов перестала фиксироваться.

На основании отчетов InfoWatch, можно выделить основные виды угроз:

1. Халатность и невнимательность сотрудников. В данном пункте речь идет о сотрудниках, которые не подозревая об этом, могут занести вирусы на сервер организации. Такая ситуация может произойти из-за открытого фишингового письма на почте, зараженного вирусом, с помощью которого злоумышленники получают доступ к любой информации, хранящейся на сервере компании.

2. Использование нелицензионного программного обеспечения. Обладатель пиратского программного обеспечения не получает технической защиты, а также актуальных обновлений программы от разработчика. Именно по этой причине важно понимать, что в таком случае у пользователя нет должной защиты от мошенников, которые намерены получить данные с сервера с помощью занесенных вирусов. По данным исследований Microsoft, около 7% проверенных нелицензионных программ имели вирусы, с помощью которых злоумышленники могли получить доступ ко всем паролям и засекреченным файлам пользователя, которыми могут быть как бухгалтерские документы, так и документы, являющимися секретными.

3. Вирусы. Одной из самых опасных и распространенных видов атак являются компьютерные вирусы. Из-за их атак организации могут понесли многомиллионный ущерб. Пути их проникновения очень разнообразны, но самым часто встречающимся до сих пор является почта (как личная, так и корпоративная). Причем, в отличие от халатности сотрудников, открывающие фишинговые письма, с вирусом это может произойти даже если пользователь не открыл письмо. Также, помимо почтовых ящиков вирусы могут проникнуть и через мобильные устройства, коммутаторы, маршрутизаторы, межсетевые экраны и так далее. За последнее время появилось много различных трояноввымогателей (англ. ransomware), которые делятся на шифровальщиков и блокировщиков. Вирусы-шифровальщики действуют на конкретные файлы компьютера, не давая возможность их открыть, а блокировщики в целом закрывают доступ ко всему компьютеру. По данным Intel распространенным вирусом-шифровальщиком WannaCry заразились около 530 тысяч компьютеров, а суммарный объем финансовых потерь компаний составил более 1 миллиарда долларов.

4. DDoS-атаки (Distributed-Denial-of-Service) или «распределенный отказ от обслуживания». Это хакерская атака на ресурс путем создания ложных потоков до того состояния, пока выбранный хост не выйдет из строя. В основном применяется для борьбы с конкурентами или для отвлечения внимания системных администраторов от другого

вида атак. Чаще всего DDoS-атакам подвергаются банковские системы (в 49% случаях), так как «распределенный отказ от обслуживания» отвлекает внимание персонала на себя, в то время как злоумышленники крадут данные или денежные средства со счетов.

5. Инсайдерские утечки информации. Это утечки информации из-за совладельцев компании. Именно легальные пользователи – основная причина потери контроля над данными в России. Инсайдеров делят на группы, такие как:

5.1. «Кроты» - сотрудники компании, тайно работающие на компанию-конкурента. Крадут важные данные для конкурента за денежное вознаграждение.

5.2. «Уволенные» - сотрудники компании, которые забирают с собой информацию, к которой сами имели доступ для того, чтобы пользоваться ею же на новом месте работы, которой могли быть засекреченные данные организации, в том числе связанные с финансовыми активами.

5.3. «Нарушители» - топ-менеджеры и среднее звено компании. Этот вид относят к непредумышленным утечкам, так как сотрудники обычно по своей невнимательности или халатности пользуются личной почтой или, например, совершают онлайн-покупки с рабочего компьютера. Именно такими путями вирусам или атакам проще и быстрее всего попасть на ресурс.

5.4. «Преступники» - в основном это топ-менеджеры или сотрудники, имеющие доступ к важной информации, которые целенаправленно отправляют и пересылают секретную информацию заинтересованным в ней третьим лицам с целью получения экономической и финансовой выгоды.

5.5. «Законодательные перипетии» - государственные или судебные органы Российской Федерации имеют полномочия изъять или конфисковать электронные носители организации в ходе проверки или судебного следствия. Так как большая часть информации хранится в электронном формате, организация не может полноценно существовать и работать. Простои в данном случае не компенсируются, а в случае продление экспертизы организация может понести большие финансовые потери и в конечном счете прекратить свою деятельность.

Существует, также и иная, более общая классификация всех возможных угроз информационной безопасности[12]:

1) по характеру возникновения;

[12] Угрозы информационной безопасности. Построение систем защиты от угрозы нарушения конфиденциальности информации. Защита информации от утечки по техническим каналам // Портал электронных систем обучения. – Екатеринбург., 2021. – С. 47-50.

1.1) объективные процессы, чрезвычайные ситуации, явления стихийных бедствий, то есть все, что не зависит от действий человека;

1.2) угрозы, происходящие непосредственно по вине человека (конкуренты, поставщики, сотрудники организации);

2) по направлению преследуемого умысла;

2.1) непреднамеренные опасности и угрозы, которые могут быть вызваны как ошибкой в процессе работы, так и небрежным отношением персонала к угрозе (не полная осведомленность о протекающих информационных процессах, установка или удаление важных инструментов обеспечения информационной безопасности, случайное повреждение каналов связи);

2.2) преднамеренные опасности и угрозы (целенаправленные действия хакеров или мошенников в информационной среде, направленные на изъятие, изменение или незаконную передачу информации);

3) по территориальному местоположению источника опасности и угроз;

3.1) опасность или угроза находится вне помещения с автоматизированной системой. К ним относятся дистанционная несанкционированная передача файлов;

3.2) опасность или угроза находится в помещении с автоматизированной системой. К ним относятся кража или несанкционированная передача файлов с записями, копиями или оригиналами документов и так далее;

3.3) опасность или угроза, источник которых находится непосредственно в автоматизированной системе. К ним относится неправильное использование инструмента;

4) по возможности проникновения к ресурсам автоматизированной системы;

4.1) угроза, которая направлена на непосредственное использования доступа к ресурсам. К ним относят несанкционированное получение ключа-пароля как при помощи кражи, так и подбором комбинаций;

4.2) угроза, которая направлена на скрытое использование пути доступа. К ним относят, нелегальный доступ к системе путем обхода встроенных средств защиты (то есть загрузка на компьютер другой пиратской операционной системы);

5) по уровню взаимосвязи угрозы и автоматизированной системы;

5.1) опасности и угрозы, которые выражаются вне зависимости от активности автоматизированной системы. К ним относят кражу физических носителей информации или вскрытие ключей криптозащиты;

5.2) опасности и угрозы, которые выражаются только в процессе обработки автоматизированных данных. К ним относят угрозы исполнения и распространения программных вирусов;

6) по актуальному территориальному расположению информации;

6.1) опасность или угроза доступа через внешние запоминающие носители информации. К ним относят несанкционированное копирование с жесткого диска или флэш-карты;

6.2) опасность или угроза доступа через внутренние средства как, например, доступ к информации на мониторе, терминале или факсе;

Вне зависимости от конкретных видов угроз или их классификации АС удовлетворяет потребности использующих ее лиц, если обеспечиваются три основных критерия информационной безопасности, а именно конфиденциальность, целостность и доступность информации.

Основные методы обеспечения информационной безопасности для устойчивой защиты данных физических лиц, организаций или государства разделяются на:

1. Базовые средства защиты электронной информации. В процессе обеспечения информационной безопасности они являются неотъемлемой частью хозяйственной деятельности любой организации или компании. К ним относят программы антивирусной защиты, системы защиты электронной почты сотрудников, которые автоматически удаляют нежелательные и подозрительные письма из почтовых ящиков. Также, нужно обеспечить работу ограниченного списка лиц, которые имеют право систематически изменять пароли и шифры.

2. Физические средства защиты информации. В данном случае речь идет о территориальной защите всей организации и отдельных особо охраняемых зон внутри помещения. К ним относят контрольно-пропускные пункты на въезд, идентификационные разрешения на вход в особо охраняемые и секретные помещения. То есть, при такой системе есть определенный перечень лиц, которым разрешено войти в помещение и посторонние лица легально войти внутрь не смогут. Часто для такого контроля используют карты HID.

3. Резервное копирование данных. В конкретном методе главный смысл в том, что для того, чтобы в случае утечки информации не потерять ее полностью и иметь возможность организации функционировать необходимо хранить информацию не только непосредственно на компьютере, но и на внешних носителях или на сервере. В случае конфискации документации или других важных информатизированных данных организация сможет не приостанавливать работу и иметь доступ ко всем своим документом. Наиболее удобным является хранение информации в «облаке». С ее помощью у пользователя есть возможность в любое время и в любом месте

воспользоваться своими данными без фактического нахождения в помещении с автоматизированной системой.

4. Анти-DDoS. Здесь необходимо понимать, что самую полную защита от DDoS-атак могут обеспечить только разработчики программного обеспечения путем вшивания этой услуги непосредственно в ПО. Эта услуга самостоятельно распознает и блокирует все опасные операции, которые приходят извне. Самостоятельная защита от такого вида атак невозможна, так как пользователь понимает, что DDoS-атаки совершаются только после получения неблагоприятного события. Главное преимущество такой защиты в том, что все процессы в организации проходят беспрепятственно и без сбоев. Данная услуга будет работать вплоть до того момента пока пользователь не сменить программное обеспечение.

5. Шифрование данных электронной информации. В данном случае для засекречивания передаваемой информации пользователям необходимо пользоваться программами-шифровальщикаци, которые, в свою очередь, позволяет подтвердить личность и подлинность информации при передаче или хранении, которая передается по каналам связи от нелегального доступа и краже.

6. Аварийное восстановления данных. Необходимо всегда иметь план действий на случай потери данных или доступа к ним для того, чтобы избежать простоя производства или деятельности организации. Данный метод может обеспечить организации сокращение времени ожидания восстановления доступа к информации.

В соответствии с рисунком 2 наглядно прослеживается структура методов и принципов информационной безопасности.

Рисунок 2 – Инфраструктура информационной безопасности[13]

[13] Понятия экономической и информационной безопасности // Открытая библиотека учебной информации. – М., 2021. – С. 13-15.

Таким образом, защита информации должна работать бесперебойно, постоянно подстраиваясь под изменения систем, а также в комплексе и взаимосвязано друг с другом, чтобы захватить все направления возможных угроз. Для того, чтобы специалисту сделать максимально устойчивое и безопасное состояние организации на рынке, необходимо использовать все вышеперечисленные методы.

Специалист по компьютерной или информационной безопасности – это профессионал в области IT-технологий, который обеспечивает целостность и конфиденциальность информации путем тестирования системы на предмет наличия уязвимостей, а также детально прорабатывая все выявленные проблемы с помощью защитных программ.

Для обеспечения информационной безопасности компаний и государства внутри организационной структуры создаются отдельные департаменты или комитеты по защите информации, где работают специалисты. Они, также, делятся на более узкие специальности, такие как[14]:

1. Пентестеры. Их еще называют «этичными» хакерами. Они на законных основаниях взламывают систему заказчика и таким образом ищут уязвимости, которые впоследствии устраняют совместно с разработчиками.

2. Специалисты по разработке. Они участвуют в процессе создания программ и приложений. Специалисты работают только с готовыми кодами и ищут в них ошибки и возможные каналы утечки информации.

3. Специалисты по сетям. Они занимаются поиском возможных и известных уязвимостей в оборудовании и сетевых системах. Проще говоря, они знают, как преступник может попасть на ваш компьютер с помощью Windows, Linux или других систем и установить необходимое программное обеспечение. Они могут как найти возможность взлома, так и создать систему, в которую будет сложно проникнуть.

1.3 Специфика организации информационной безопасности в органах государственного управления

Сегодня важно отметить еще одну тенденцию как за рубежом, так и в России - разработку и внедрение концепций электронного правительства, основанных на

[14] Mueller J. P. Security for Web Developers: Using javascript, HTML, and CSS / J. P. Mueller - O'Reilly Media, 2015 – 384 p.

использовании информационных технологий при создании государственных источников информации и доступе к информации для граждан и пользователей о деятельности государства.

В Российской Федерации существует три основные базовые модели электронного правительства, которые делятся на:

1. Государство для граждан – это отношения, которые возникают между государственными и муниципальными образованиями и непосредственно гражданами.

2. Государство для бизнеса – это отношения, которые возникают между государственными и муниципальными образованиями и участниками ведения бизнеса в стране.

3. Государство для государства – это отношения, возникающие внутри государственного аппарата между различными ведомствами.

Говоря о модели «государство для граждан» основными действиями, направленными на гражданское общество, является оказание государственных услуг в электронном виде. Это может быть выдача какого-либо документа, получения справок, выплата гарантий и так далее. Основным порталом, предоставляющим такого вида услуги, является «Госуслуги», функционирующий на территории страны с 2009 года. По данным портала на 31 декабря 2019 года, количество зарегистрировавшихся на нем людей превысило 100 миллионов человек. Несомненно, использование интернет-портала по оказанию базовых государственных услуг в любое время и в любой точке земного шара очень удобно (чем и вызван спрос), однако, учитывая проблемы цифрового неравенства граждан, а также не соблюдение элементарных правил по соблюдению информационной безопасности, множество людей отказать использовать цифровизованную модель правительства.

В модели «государство для бизнеса» основной идеей является проведение закупок, получение доступа к открытым данным и участие в обсуждении проектов нормативно-правовых актов. Закупки проводятся через специально для этого предназначенном официальном государственном сайте. Самым важным аспектом в данной модели является возможность получения доступа к открытым данным, так как таким способом граждане и бизнес могут не только убедиться в прозрачности деятельности власти, но и использовать их в своих законных целях и интересах. Таким образом, данная описываемая модель имеет полноценную инфраструктуру и развивается в правильном направлении.

Модель «государство для государства» включает в себя прежде всего внутренний ведомственный документооборот. Главная цель данной модели состоит в том, что при использовании специального программного обеспечения есть возможность

централизовано хранить информацию и передавать ее в другие ведомства посредством информационных технологий. Для решения возникающих проблем с перегрузкой каналов или периодическими кибер-атаками была создана Единая сеть передачи данных.

На сегодняшний день международные концепции электронного правительства так же разделены на 4 основные модели их построения: русская, азиатская, европейская и англо-американская модели.

Азиатская модель электронного правительства получила распространение в Сингапуре и Южной Корее. Основной целью ее введения законодательство стран считает удовлетворение потребностей граждан в информационном виде в сферах культуры и образования. Также, она была создана для упрощения процедуру обучения и переквалификации. Данная система была признана Организацией Объединенный Наций самой удобной и эффективной по всему миру. Основная задача – это обеспечение государственными услугами через режим единого окна, с помощью которого максимально снижается потребность в прямом контакте между гражданином и государством, и все услуги можно получить в одном месте. Это было создано исключительно для удобства граждан, и данная разновидность электронного правительства успешно применяется. В Сингапуре был создан интернет-портал под названием «Электронный гражданин», по аналогии с которым впоследствии в России был создан портал «Госуслуги». В свою очередь, Южная Корея стала первой страной, которая ввела полный документооборот внутри страны, благодаря чему у них получается экономить более 1 миллиарда долларов ежегодно. Однако, самые ценные данные хранятся еще и в бумажном виде. Также, положительным решением для максимального удобства граждан стала установка терминалов по оказанию государственных услуг по городам в места наибольшего скопления людей (площади, остановки общественного транспорта и так далее).

Таким образом, азиатская модель успешно и на достойном уровне обеспечивает всю необходимую информацию при помощи внедрения системы электронного правительства в культурную сферу, сферу образования и здравоохранения. Также, данную систему интегрируют не только для компьютерного программного обеспечения, но и для мобильных устройств для наиболее простого контакта с субъектами, осуществляющих необходимые для гражданина услуги.

Европейскую модель электронного правительства применяется в подавляющем большинстве стран Центральной, Западной и Восточной Европы. Основная цель – это обеспечение граждан возможностью исполнять свой гражданский долг, голосуя в режиме онлайн, оказание помощи правительством в процессе уплаты налоговых отчислений и

оплаты штрафных санкций, а также предоставление информации о деятельности правительства в режиме онлайн. Отличительной особенностью модели является полный контроль и регулирование на законодательном уровне всех информационных потоков, происходящих на территории стран. Также, особенность именно этого метода заключается в объединении всех стран и наций, входящий в их состав путем введение единой валюты и осуществления единой государственной политики для обеспечения равноправия. Однако, процесс получения услуг в странах Европы не такой простой как в азиатской модели, что и является главной проблемой, особенно среди молодежи. В начале XXI века была введена система под названием «Электронная Европа».

Например, в Германии система «Электронная Европа» является катализатором деятельности по обеспечению модернизации государственного аппарата и протеканию всех процессов «государство для граждан». Это стало принципиально новой моделью обеспечения государственной власти, благодаря чему деятельность аппарата стала намного прозрачнее, а также система позвонила гражданам стать стратегическими партнерами государства и дала им возможность участвовать в процессах высказывания предложений при подготовке государственных решений.

Таким образом, европейская модель электронного правительства в большинстве своем связана на построении единства народов Европы. Она позволяет гражданам лично видеть и принимать участие в публичных дебатах, а также слушаниях по вопросам государственного устройства. Модель довольно успешно развивается, даже учитывая контроль государства за всеми потоками информации среди стран Европейского Союза.

Англо-американская модель электронного правительства применяется в таких странах как Канада, Великобритания и США. Основная цель модели – это открытость и прозрачность государства перед гражданами, а также внедрение упрощенной системы коммуникации между участниками бизнес-процессов и гражданами относительно государственного аппарата. Отличительными чертами англо-американской модели являются полная реструктуризация и реформа всей существующей модели государственного управления, использование направление деятельность на внешнюю политику и общение сотрудников государственных организаций с гражданами непосредственно через созданные порталы и системы, а не лично. Однако, в США все еще сохраняется довольно низкий уровень развития электронного правительства в сравнении с Канадой и Великобританией. Для решения этой проблемы был создан документ под названием «Стратегия электронного правительства», в котором заложен мотив предоставления гражданам США наиболее понятных и эффективных процедур получения государственных услуг.

В 1994 году Канада стала одной из первых стран мира, которая предприняла меры по созданию открытого доступа к информации со стороны государственных органов, в результате чего был создан сайт правительства, а также различные программные обеспечения, выполняющие полный документооборот внутри страны.

Таким образом, англо-американская модель имеет свои недостатки в виде низкого уровня развития электронного правительство в США. Однако, благодаря созданной системе странам удалось значительно снизить расходы на обеспечения государственного управления на местах.

Российская же модель электронного правительства применяется и действует только на территории Российской Федерации. Основная преследуемая цель создания была в совершенствовании исходного процесса обеспечения коммуникации между государственными органами и населением, а также повешения уровня качества предоставляемых услуг и доступности для населения. Переход к системе электронного правительства начался еще в 2002 году после принятия программы «Электронная Россия». С ее помощью был создан начальный нормативно-методический вариант для создания и внедрения системы электронного правительства. После этого была создана программа «Информационное общество», которая была прописана до 2020 года и должна была усовершенствовать имеющуюся нормативную базу. В Международном индексе развития электронного правительства, разработанного Организацией Объединенных Наций за 2020 года Россия заняла 36 место, однако в предыдущем периоде была на 4 позиции выше. На снижения уровня повлияла недостаточная финансовая поддержка мероприятий, которые были направлены на совершенствование информационно-технического обеспечения системы электронного правительства.

Опыт внедрения моделей электронного правительства в развитых странах показывает, что гражданам предоставляется реальная возможность вести диалог с властями, влиять на важные правительственные решения, представлять собственные инициативы, получать подробную информацию о работе государственных органов и осуществлять контроль над их деятельностью.

Создание электронного правительства с разными моделями подразумевает решение общих проблем, возникающих в обществе:

1) организация электронного документооборота в правительстве;

2) максимальный перевод отношений между государством и гражданским обществом в электронный вид;

3) использование Интернета для организации интерактивного общения власти и населения.

Практическая реализация поставленных государством задач позволит не только сразу получить информацию о мнении населения о наиболее важных решениях правительства, но и эффективно реализовать идею непосредственного участия и активизации граждан. гражданская позиция в решении важнейших проблем современного мира.

Таким образом, большинство зарубежных стран начали переход к информатизированным системам электронного правительства еще в 20 веке и на данный момент добились значительных успехов в качестве и доступности предоставляемой информации как резидентам, так и нерезидентам страны. Россия, учитывая успешный зарубежный опыт применение системы, также находится на стадии совершенствования имеющихся порталов и ресурсов для улучшения и ускорения предоставляемой информации.

2. Инструменты управления и способы обеспечения информационной безопасности

2.1 Состояние информационной безопасности в Российской Федерации

Задачи в области информационной безопасности в России - это лишь часть глобальных задач и проблем. Общий коэффициент угроз в мире показывает, что Россия находится на втором месте по количеству кибертеррористических и хакерских атак. При этом 41% всех хакерских атак в мире происходит в США, в России - не более 10%. Текущая ситуация позволяет использовать относительно комфортный режим и направлять силы для повышения уровня защиты от предполагаемых угроз.

В России все аспекты борьбы с угрозами информационной безопасности на национальном уровне оцениваются на уровне Доктрины информационной безопасности, которая служит основой для принятия нормативных актов. Ключевые вопросы Доктрины включают потребность России в независимом информационном присутствии в международном сообществе и выбор каналов для предоставления надежных данных и отчетов, которые уменьшают ущерб, наносимый дезинформирующими атаками.

Что касается качества управления государством или компанией, то уровень информационной безопасности определяется способностью субъекта[15]:

1) обеспечить функционирование информационных ресурсов и потоков, достаточных для нормальной жизни и развития;

2) полностью защищать коммерческую или государственную тайну от незаконного вмешательства;

3) противостоять техническим и психологическим угрозам, защищать систему и пользователей от негативных воздействий с помощью информационных технологий;

4) поддерживать эффективность работы, «саморазвитие» и верные системные ответы на растущие вызовы;

5) использовать методы и средства защиты информационного суверенитета государства или корпоративных ценностей, не нарушающие целостность прав и свобод других государств и граждан.

В настоящее время за информационную безопасность в России отвечают различные государственные учреждения, в том числе Федеральная служба по техническому и экспортному контролю (ФСТЭК), Федеральная служба по надзору в

[15] Лопатин Ю. Н. Информационная безопасность в России. Проблемы, поиски решений // Информационная безопасность в России. 2018. №2. С. 51-52.

сфере связи, информационных технологий и массовых коммуникаций (Роскомнадзор) и специализированные управления министерств, непосредственно министерства, а также межведомственная комиссия при Совете Безопасности. Однако участники процесса кибератак считают, что на данном этапе необходимо объединить функции и передать их отдельному регулятору на уровне федеральных служб с независимыми ресурсами и значительными полномочиями.

Российская система все еще находится в стадии развития и не отвечает всем требованиям, необходимым для обеспечения полной информационной безопасности. Причин несколько:

1. Независимость. Независимость или степень локализации систем, необходимых для функционирования государства, обеспечивается посредством собственного программного обеспечения – операционных систем, систем защиты информации (лучшими операционными системами России признаны Alt Linux, Astra Linux и Ось); собственных каналов связи для поддержания «автономности» важнейших ресурсов от глобальной сети Интернет, а также квалифицированных кадров (по подсчетам Минкомсвязи в 2020 году произошел рост количества квалифицированных специалистов в области информационной безопасности и составил 350 тысяч человек). Важным аспектом обеспечения независимости является создание хорошо отлаженной системы межведомственного взаимодействия и независимой структуры управления рисками, основанной на нормативно-правовой базе, которая обеспечивает полномочия и возможности бесперебойной работы. Существенной проблемой является отсутствие собственного оборудования, что ставит российскую систему защиты информации в зависимость от зарубежных поставщиков.

2. Слабая защищенность финансовой системы. С марта по ноябрь 2020 года Центр мониторинга и реагирования на компьютерные атаки в кредитно-финансовой сфере (FinCERT) зафиксировал не менее 20 масштабных кибератак на платежные системы. Злоумышленники пытались украсть у российских банков 2,87 миллиарда рублей. Совместно с отделами информационной безопасности банков и правоохранительными органами удалось предотвратить хищение более 1,5 млрд рублей.

3. Несовершенство информационной безопасности в социальной сфере. Главной целью является реализация высокого уровня обеспечения безопасности информации в таких сферах жизни как образование и социальная. Основополагающая проблема здесь содержится в том, что Российская Федерация не обладает достаточным уровнем среди международных сообществ и не может контролировать мировые социальные сети. В первом случае проблема заключается в том, что принцип давления на крупнейшие

источники с просьбами предоставить личные данные пользователей не всегда работает. В последнем случае необходима координация между различными ведомствами, так как эта проблема не может быть решена силами МВД и Роскомнадзора в одиночку. За последние 2 года Роскомнадзор заблокировал 17 000 доменных имен и пользователей, но они снова появляются - под другими именами, но с тем же кругом подписчиков.

4. Проблемы и угрозы на международном уровне. Информационные угрозы в России и в мире имеют прежде всего экономическое «происхождение». Кибертерроризм, направленный на подрыв политической стабильности, встречается реже и его очевидные масштабы объясняются широким освещением в СМИ. Кроме того, громкие взломы часто носят «рекламный» характер и служат своеобразной презентацией услуг той или иной хакерской группы, которая планирует применить свои способности и возможности на коммерческом «конвейере». Публичные действия также выполняют разведывательные функции. Таким образом, хакеры определяют степень защиты мировых информационных ресурсов и готовятся к новым, более серьезным и масштабным операциям. По данным Центра стратегических и международных исследований США, ежегодный ущерб от кражи компьютерной информации во всем мире превышает 440 миллиардов долларов.

Эксперты по информационной безопасности отметили основные тенденции рынка информационной безопасности в России и спрогнозировали развитие киберугроз и средств защиты информации на 2021 год. Были затронуты темы удаленной работы и рисков утечки данных, машинного обучения и искусственного интеллекта, а также безопасности как услуги. Ожидается рост киберпреступности и атак, в том числе атак на критически важные инфраструктуры. В таких условиях особенно важно использовать продукты и решения безопасности, отвечающие требованиям, реализовать автоматизацию информационной безопасности и усилить аутентификацию удаленных пользователей.

Главная проблема заключается в том, что из-за разрозненной и разнообразной инфраструктуры формируется более широкий фронт атаки. Это происходит из-за вынужденного режима удаленной работы, возникшего в 2020 году непосредственно в результате пандемии. Сюда входит, в частности, большая проблема защиты «домашних офисов» - рабочих мест людей, работающих удаленно. Также, из этой проблемы вытекает и проблема утечки данных. Системы безопасности России не были готовы к резкой смене работы большей части корпораций на удаленную, вследствие чего в 2020 году был выявлен большой всплеск утечек различных данных.

В последние годы были предприняты определенные практические меры по усилению информационной безопасности в Российской Федерации. Началось формирование нормативно-правового обеспечения информационной безопасности -

приняты законы «О безопасности» и «О государственной тайне», начата работа по созданию механизмов их реализации и завершена подготовка законопроектов, регулирующих деятельность в информационной сфере. В дополнение к имеющимся, 12 апреля 2021 был издан указ Президента «Об утверждении Основ государственной политики Российской Федерации в области международной информационной безопасности», который направлен на:

1) продвижение на мировой арене российских подходов к формированию системы обеспечения информационной безопасности и российских инициатив;

2) содействие созданию международно-правовых механизмов предотвращения (урегулирования) межгосударственных конфликтов в глобальном информационном пространстве;

3) организацию межведомственного взаимодействия при реализации государственной политики в области международной информационной безопасности[16].

В соответствии с рисунком 3 можно увидеть, что по состоянию на конец 2020 года количество уникальных киберинцидентов увеличилось на 51% по сравнению с 2019 годом. Семь из десяти атак носили конкретный целенаправленный характер. По мнению киберпреступников, наиболее интересными отраслями являются государственные и медицинские учреждения и промышленные предприятия. В связи с пандемией COVID-19 частота взлома при атаках на организации выросла. По итогам 2020 года доля данного метода составляет 24% (на 10 процентных пунктов больше, чем в 2019 году). Медицинские учреждения занимают первое место по количеству атак с использованием шифров и третье место по количеству атак в год. Из-за действий хакеров медицинские системы оказались недоступными, а больницам даже пришлось отказывать пациентам в оказании неотложной помощи. Количество атак на промышленных предприятиях увеличилось на 91% по сравнению с 2019 годом, а доля взлома увеличилась в 2,6 раза по сравнению с предыдущим годом. Сообщалось о нападениях на критически важные объекты инфраструктуры, приводящих к отключению электроэнергии, а также о попытках взлома систем водоснабжения.

[16] Об утверждении Основ государственной политики Российской Федерации в области международной информационной безопасности : утв. указом Президента РФ от 12 апреля 2021 №213 // КонсультантПлюс : справ. Правовая система. – Версия проф. – М., 2021. – Режим доступа : локальная сеть Науч. б-ки Том. гос. ун-та.

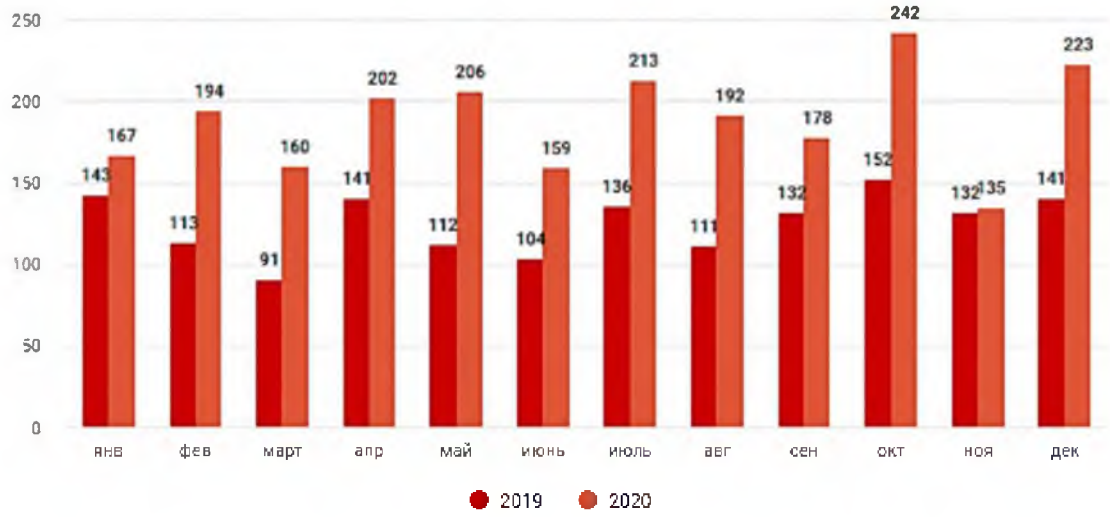

Рисунок 3 – Количество инцидентов кибератак в сравнении 2019 и 2020 годов[17]

Таким образом, российская система обеспечения информационной безопасности все еще находится на стадии развития и не отвечает всем требованиям, необходимым для обеспечения полной информационной безопасности. В этом, несомненно, есть и вина пандемии, из-за которой весной 2020 года большей части компаний пришлось экстренно перевести сотрудников на удаленный режим работы, из-за чего выяснилось, что российские системы безопасности не были готовы к такому скорому переходу к информатизированным системам.

2.2 Отечественный опыт обеспечения и управления информационной безопасностью

Государственные учреждения, оборонная промышленность, коммерческие корпорации, финансовые учреждения, медицинские учреждения и малые предприятия регулярно собирают большие объемы конфиденциальных данных о персонале, клиентах, конкурентах, продуктах и финансовом обороте.

Защита информации предоставляется в любом государстве и проходит множество этапов в своем развитии, в зависимости от потребностей государства, возможностей, методов и средств ее получения (особенно разведки), правового режима государства и его реальных усилий по обеспечению информационной защиты.

[17] Актуальные киберугрозы: итоги 2020 года. [Электронный ресурс] // Positive Technologies – М., 2021. - URL: https://www.ptsecurity.com/ru-ru/research/analytics/cybersecurity-threatscape-2020/ (Дата обращения 12.05.2021).

Важным этапом в становлении и совершенствовании такой системы в нашей стране стал период 1970-1980 годов. С начала 70-х гг. широкое использование технических средств для исследований началось в разведывательной деятельности мировых лидеров. 1980-е годы, отмеченные бурным научно-техническим прогрессом, особенно в военной области, дали новый импульс расширению возможностей внешней разведки: до 70% информации было добыто техническими средствами. Борьба с технической разведкой стала одной из составляющих общей системы мер по защите государственной и служебной тайны[18].

Государственная техническая комиссия СССР была создана постановлением правительства от 18 декабря 1973 года для организации и координации работ в этой области. В то же время начала формироваться система научного обеспечения комплексных действий против иностранных служб технической разведки. Высшие государственные органы Российской Федерации предприняли ряд важных шагов. В частности, Указом Президента РФ от января 1992 г. на базе Государственной технической комиссии СССР создан государственный орган высшего статуса - Государственная техническая комиссия под руководством Президента Российской Федерации (Гостехкомиссия России)[19].

В настоящее время происходят серьезные изменения в методологии защиты информации. Происходит переход от дорогостоящего сокрытия намеренно завышенных данных к гарантированной защите критических «узлов». Заложены правовые основы для этой деятельности. Принят Закон Российской Федерации «О государственной тайне» и Федеральный закон «Об информации, информатизации и защите информации». Указанные нормативно-правовые акты были созданы с целью считывания интересов личности, общества и государства.

Одним из инструментов регулирования обеспечения информационной безопасности как на государственном уровне, так и на уровне предприятий и граждан является нормотворческая деятельность. Законодательная база в сфере обеспечения безопасности информационных данных выделена в отдельную подотрасль базы законодательства информационной сфере.

В настоящее время существует программа, направленная на усовершенствование

---

[18] Косовец А. А. Информационная безопасность в системе обеспечения экономической и национальной безопасности России // Вестник Академии экономической безопасности МВД России. Право. – 2011. - №2. – С. 20-22.

[19] Бабаш А. В. Информационная безопасность. История защиты информации в России [Текст] : [учебное пособие] / А. В. Бабаш, Е. К. Баранова, Д. А. Ларин. - Москва : КДУ, 2013. - 735 с.

существующей модели информационной безопасности. Ее положения были одобрены в 1998 году на парламентских слушаниях в Государственной Думе Российской Федерации и на заседании Комитета Государственной Думы по безопасности, благодаря которым было принято не менее 20 новых законодательных акта. Межведомственная комиссия Совета Безопасности Российской Федерации по информационной безопасности в свою очередь обозначила, что уровень современной информационной безопасности не подходит под критерии международного уровня, тем самым утвердила следующие направления развития законодательства[20]:

1. Внесение изменений в действующее законодательство в целях уничтожения разногласий со стандартами Конституции Российской Федерации и интернациональных соглашений, к коим присоединилась Россия, коллизий меж законодательными актами федерального значения и актами, учреждающими органы работа по обеспечению информационной защищенности Российской Федерации (в ст. 5 Закона «О международных договорах» 1995 г. говорится о том, что если международным договором Российской Федерации установлены иные правила, чем предусмотренные законом, то применяются правила международного договора, однако уже с 1 июля 2020 года в новом тексте поправок к Конституции говорится о том, что решения межгосударственных органов, принятые на основании положений международных договоров Российской Федерации в их истолковании, противоречащем Конституции Российской Федерации, не подлежат исполнению в Российской Федерации)[21].

2. Разработка Государственной программы становления общественных компьютерных сетей, охватывая определение правового статуса интернет-провайдеров и правовое регулирование их работы, передача информации в сети Интернет о работе органов государственной власти и районного самоуправления, защита российского языка в Интернете.

3. Создание нормативно-правовой базы для становления системы страхования информационных рисков, направленной на гарантированное страховое покрытие пользователей, оставивших информационные предложения и лиц, предоставляющих эти предложения, объяснение правового статуса зарубежного инвестора в сфере вложений и связи в целях обеспечения государственной защищенности Российской Федерации.

---

[20] Вопросы Совета Безопасности Российской Федерации : утв. указом Президента РФ от 06.05.2011 N 590 (ред. от 07.03.2020 // КонсультантПлюс : справ. Правовая система. – Версия проф. – М., 2021. – Режим доступа : локальная сеть Науч. б-ки Том. гос. ун-та.

[21] Конституция Российской Федерации: принята всенародным голосованием 12.12.1993 с изменениями, одобренными в ходе общероссийского голосования 01.07.2020 от 14 марта 2020 г. N 1-ФКЗ) / Собрание законодательства Российской Федерации. – 2020. – Ст. 79.

4. Законодательное разграничение уровней правового регулирования проблем информационной безопасности (федеральный уровень, уровень субъектов Федерации, уровень местного самоуправления).

5. Законодательное закрепление приоритета развития национальных сетей связи и отечественного производства спутников для космической связи.

6. Правовое регулирование развития негосударственной составляющей в формировании информационного общества и обеспечении информационной безопасности России.

7. Создание правовой основы функционирования системы региональных центров защиты информации в Российской Федерации.

В последние годы очевидные сдвиги в данной сфере возможно отследить под воздействием процессов информатизации. Правовой почвой считается Федеральный закон «Об информации, информатизации и обороне информации», который четко регулирует вопросы правового режима источников информации. На основании положений обозначенного Федерального закона сотворена нормативно-правовая основа информатизации физических лиц Российской Федерации.

Преодоление отставания от передовых стран требует организации и стимулирования производства. В этом блоке проблем особого внимания заслуживают следующие вопросы:

1) программирование и создание продуктов по мировым стандартам, особенно для открытых информационных бизнес-систем;

2) регулирование отношений в сфере информационной деятельности, информационных услуг, организация и обеспечение ответственности различных посреднических структур в информационно-коммуникационных системах;

3) формирование рынка информационных продуктов.

Говоря об обеспечении и регулировании информационной безопасности организаций необходимо учитывать специфику конкретных бизнес-процессов. На практике обеспечение информационной безопасности компаний осуществляется следующими способами (рисунок 4):

Рисунок 4 – Основные способы для реализации информационной безопасности[22]

1. Моральные средства защиты. Под ними понимают стандарты поведения и правила работы с информационными активами, которые возникли в результате распространения и внедрения электронных технологий в различных секторах государства и общества в целом. Фактически, это необязательные требования, в отличие от законодательных. Однако их нарушение приведет к потере репутации человека и организации. Моральные и этические средства защиты информации должны в первую очередь включать честность и порядочность сотрудников. В каждой организации есть свой набор правил и положений, направленных на создание здорового морального климата в коллективе. Механизм безопасности - это внутренний документ компании, учитывающий специфику бизнес-процессов и структуры информации, а также структуру IT-системы.

2. Организационные средства. Регулируют работу системы обработки информации, сотрудников организации и процесс взаимодействия их с системой, чтобы устранить или предотвратить угрозу информационной атаки или снизить потери в случае их возникновения. Основная цель - установить внутреннюю политику конфиденциальности засекреченных данных, включая использование и контроль необходимых ресурсов. Реализация политики конфиденциальности включает в себя выполнение контрольных и технических задач, а также набор сотрудников внутренней безопасности. Возможны изменения в структуре IT-системы, поэтому системные администраторы и программисты должны участвовать в реализации политики конфиденциальности. Все сотрудники компании должны быть обучены правилам работы с конфиденциальной информацией.

3. Правовые средства. Они основаны на законах, решениях и нормативных актах, действующих в Российской Федерации, которые устанавливают правила обработки

[22] Бирюков А. А. Информационная безопасность: защита и нападение. – 2-е изд., перераб. и доп. – Москва : ДМК Пресс, 2017. – 434 с.

персональных данных, гарантируют права и обязанности участников работы с источниками информации при их обработке и использовании, а также ответственность за нарушения этих правил, что устраняет угрозу несогласованного использования конфиденциальной информации. Такие правовые приемы используются как превентивные меры. По сути, это организованные объяснительные беседы с сотрудниками компании, использующими электронные устройства компании.

4. Программные средства. Безопасность сети обеспечивается специальными программами, защищающими источники информации от несанкционированных действий. Программные методы защиты конфиденциальных данных благодаря своей универсальности, простоте использования и настройки являются наиболее популярными. Однако это делает их уязвимыми элементами информационной системы предприятия. Сегодня создано большое количество антивирусных программ, брандмауэров и средств защиты.

Наиболее распространенными на сегодняшний день антивирусами, брандмауэров и средствами обнаружения вторжений являются:

1) антивирусное программное обеспечение, предназначенное для обнаружения вирусных атак. Наиболее известны TrendMicro, Symantec, Network Associates;

2) средства обнаружения атак. Самые популярные на рынке – это Symantec и Entercept Security Technology;

3) брандмауэры (межсетевые экраны), которые контролируют все коммуникации в локальной сети и действуют как фильтр или прокси-сервер. Они используют стандарты ITSEC (Схема оценки и сертификации безопасности информационных технологий) и IASC (Услуги по информационной безопасности и сертификации). Популярными представителями рынка являются Microsoft, Checkpoint Software, Net Screen Technologies, Cisco Systems и Symantec Corporation.

5. Аппаратные средства. Они представляют собой электронные устройства, встроенные в блоки автоматизированной системы или разработанные как независимые устройства, которые контактируют с этими блоками. Их задача - внутренняя защита структурных компонентов IT-систем процессоров, сервисных терминалов, вторичных устройств. Это реализовано с использованием метода управления доступом к ресурсам (идентификация, аутентификация, контроль авторизации системного объекта, регистрация).

6. Физические средства. Это разные типы механических и электронно-механических устройств для создания физических барьеров, когда злоумышленники пытаются повлиять на компоненты автоматизированной системы защиты информации.

Они также являются техническими устройствами для охранной сигнализации, связи и внешнего мониторинга. Объекты физической безопасности направлены на защиту от стихийных бедствий, пандемий, боевых действий и так далее.

7. Технические способы. Различные электронные и специализированные устройства, входящие в один автоматизированный комплекс организации и выполняющие самостоятельные и сложные функции хранения персональных данных. К ним относятся персонализация, авторизация, аутентификация, ограничение доступа к активам пользователей, шифрование.

8. Криптографические методы. Этот метод основан на методиках шифрования и обеспечивает защиту конфиденциальной информации посредством программной и аппаратной защиты информации. Криптографический метод обеспечивает высокую эффективность средств индивидуальной защиты. Его можно выразить в цифровом виде: среднее количество операций и время на разрешение ключей и расшифровку данных. Методы аппаратного шифрования используются для защиты текстов во время передачи, а программные методы также используются для обмена информацией между компьютерами в локальной сети. Для хранения информации на магнитных носителях используются методы программного шифрования. Однако у них есть определенные недостатки: время и мощность процессоров для шифрования информации, трудности с расшифровкой, высокие требования к защите ключей (угроза обмена открытыми ключами).

Учитывая существующие способы обеспечения информации, российские компании-разработчики находятся в состоянии непрерывного совершенствования и создания новых систем защиты информационной безопасности. В связи с чем, выручка крупнейших отечественных поставщиков средств защиты информации растет вслед за общим ростом IT-рынка. По итогам 2018 года суммарный оборот 30 крупнейших участников рейтинга превысил показатель прошлых лет[23]. В соответствии с рисунком 5, выручка крупнейших отечественных игроков рынка информационной безопасности выросла на 8% по итогам 2018 года и достигла 111,5 млрд. рублей, незначительно превысив рекорд 2016 года в размере 111 млрд. рублей. Рост выручки ведущих рейтинговых агентств CNews Security по итогам 2019 года достиг 37% и превысил 150 миллиардов рублей. Состав его участников значительно расширился и обновился, в том числе за счет компаний, бизнес которых связан с законом Яровой.

[23] Балановская А. В. Анализ и тенденции рынка информационной безопасности в России / А. В. Балановская, А. В. Волкодаевая // Экономические науки. 2019. №1. С. 226-229.

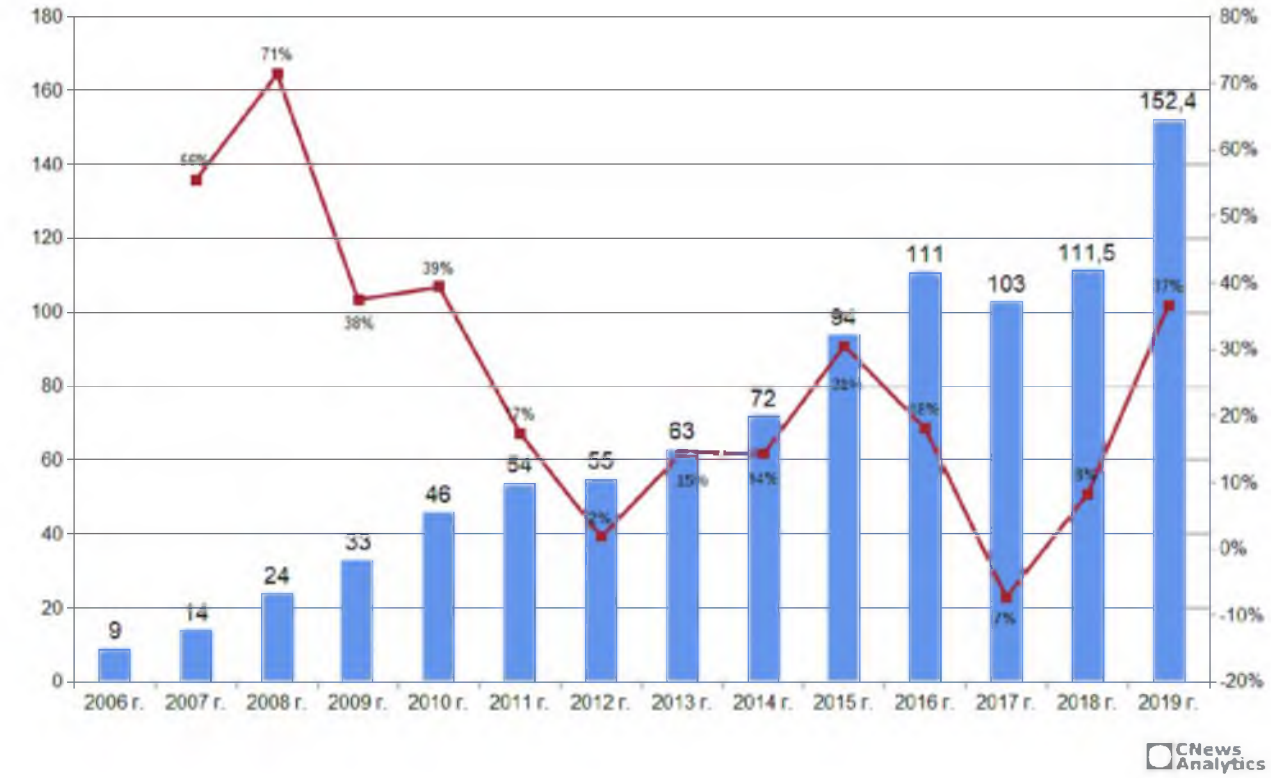

Рисунок 5 – Динамика рейтинга крупнейших поставщиков ИБ с 2006 по 2019 гг., в млрд. руб.[24]

«Закон Яровой» или «Пакет Яровой» состоит из двух законопроектов и направлен на борьбу с террористическими актами. Первый законопроект вводит в Уголовный кодекс Российской Федерации три новых состава преступления: не информирование о террористических актах, участие в экстремизме и совершение международных террористических актов[25]. Второй законопроект содержит правила о том, что интернет-компании и операторы мобильной связи должны предоставить правоохранительным органам имя, фамилию, отчество, дату рождения, паспортные данные, адрес, аудио- и видеофайлы, адрес электронной почты, текстовые сообщения и список родственников клиента.

Российские компании-производители и компании, внедряющие средства защиты в оборот ежегодно вносятся в рейтинг российских производителей средств защиты IT

[24] Аналитика. Российский рынок информационной безопасности [Электронный ресурс] // CNews. - URL: https://www.cnews.ru/reviews/security2019/articles/rossijskij_rynok_informatsionnoj (Дата обращения 26.04.2021).

[25] О внесении изменений в Уголовный кодекс Российской Федерации и Уголовно-процессуальный кодекс Российской Федерации в части установления дополнительных мер противодействия терроризму и обеспечения общественной безопасности : Федеральный закон от 6 июля 2016 г. N 375-ФЗ // КонсультантПлюс : справ. Правовая система. – Версия проф. – М., 2021. – Режим доступа : локальная сеть Науч. б-ки Том. гос. ун-та.

сферы. Он рассчитывается исходя из выручки, прибыли и стоимости отчетного года (таблица 2).

Таблица 2 - Рейтинг российских производителей средств защиты информации[26]

№	Компания	ОКВД	Выручка, тыс. руб.	Прибыль, тыс. руб.	Стоимость, тыс. руб.	Год
1	АО «Лаборатория Касперского»	Разработка компьютерного программного обеспечения (62.01)	32 499 855	9 324 762	29 622 589	2020
2	ООО «Газинформ сервис»	Деятельность по использованию вычислительной техники и информационных технологий, прочая (62.09)	8 935 788	2 089 204	2 972 222	2020
3	ООО «Код безопасности»	Производство компьютеров и периферийного оборудования (26.20)	5 853 729	1 493 953	-	2020
4	ООО «Крипто-Про»	Разработка компьютерного программного обеспечения (62.01)	2 590 428	1 221 187	1 211 383	2020
5	ООО «Серчинформ»	Научные исследования и разработки в области естественных и технических наук, прочие (72.19)	972 367	900 825	482 478	2020

В год пандемии из-за масштабного перевода множества компаний на режим удаленной работы АО «Лаборатория Касперского» продемонстрировала позитивные результаты, защищая приватность пользователей и помогая компаниям снижать риски столкновения с киберугрозами в условиях цифровизации. В России суммарные продажи компании увеличились на 16% в рублёвом эквиваленте, следовательно, увеличилась и прибыль компании, благодаря чему Лаборатория Касперского заняла первую строчку рейтинга с большим отрывом от ООО «Газинформсервис». «Лаборатория Касперского»

[26] Рейтинг российских производителей средств защиты информации [Электронный ресурс] // CISO CLUB. Информационная безопасность. - URL: https://cisoclub.ru/ (Дата обращения 26.04.2021).

продолжает предоставлять одни из ведущих продуктов и услуг для защиты своих клиентов по всему миру и достигла значительных успехов в секторах «бизнес для бизнеса» (рост 13% по сравнению с 2019 годом) и «бизнес для потребителя» (рост 4% по сравнению с 2019 годом). Результаты продаж в 2020 году были одними из лучших за всю историю компании.

Эксперты спрогнозировали пять основных тенденций, которые определят развитие российского рынка информационной безопасности на 2021 г[27]. По мнению экспертов компании, ключевые изменения в отрасли будут вызваны переходом на гибридный график, сочетающий в себе удаленную работу и офисную работу, ограниченные бизнес-бюджеты и растущую активность киберпреступников перед лицом изменений в IT-сфере:

1. Переосмысление подходов к информационной безопасности при гибридном формате работы. Информационные границы компаний станут еще более размытыми: теперь они должны включать все объекты, на которых работают сотрудники. Широкий переход к дистанционной работе изменит схемы организаций. Растет фактор географического распределения рабочих мест еще и потому, что компании, работающие на условиях удаленной работы, стали чаще нанимать сотрудников из других регионов. Для специалистов отдела информационной безопасности организации это означает необходимость защиты не только инфраструктуры, расположенной в офисах компании, но и информационных систем у сотрудников дома. Для этого важно четко понимать, какие данные хранятся на личных устройствах и каковы риски.

2. Увеличение доли информационной безопасности в IT-бюджетах российского бизнеса. Трудная экономическая ситуация имеет два пути последствий. С одной стороны, это способствует росту киберпреступной активности. С другой стороны, это ограничивает возможности роста корпоративных IT-бюджетов. В ситуации, когда технологические бюджеты компаний в среднем не растут (даже сокращаются для многих компаний), вероятно временное перераспределение бюджетов в пользу инструментов безопасности, в частности, за счет снижения затрат на разработку IT-инфраструктур.

3. Использование поведенческого анализа для защиты данных. Специалисты по информационной безопасности пришли к выводу, что не может быть единого решения для защиты общества в целом и компаний в частности от всех возможных угроз. Надежная система безопасности имеет модульную структуру и состоит из набора интегрированных решений. Средства защиты периметра и межсетевого экрана, безопасности веб-

[27] Основы государственной политики РФ в области международной информационной безопасности [Электронный ресурс] // Varonis Systems. - URL: https://www.varonis.com/ru/ (Дата обращения 26.04.2021).

приложений и предотвращения потери данных становятся необходимостью для всех крупных предприятий.

4. Развитие инструментов автоматизации. Повышенная активность киберпреступников и ограниченные ресурсы приводят к растущей потребности в технологиях, позволяющих автоматизировать работу отделов информационной безопасности. Эти инструменты включают, например, инструменты для автоматической классификации данных в соответствии с их уровнем конфиденциальности. В 2021 году также будут разработаны инструменты корреляции, позволяющие правильно находить взаимосвязь между событиями и предупреждать департаменты или отделы информационной безопасности только о действительно опасных событиях. Такие системы, с одной стороны, избавят сотрудников от контроля над большим количеством уведомлений, а с другой стороны, не пропустят действительно важные предупреждения, указывающие на потенциальные атаки.

5. Специалисты по информационной безопасности должны развивать аналитические навыки. Требования к профессионалам в области кибербезопасности существенно меняются. Директорам по информационной безопасности и их подчиненным становится недостаточным получение только технических данных и требуется все больше аналитических навыков. Чтобы построить и развить жизнеспособную систему необходимо постоянно анализировать бизнес-процессы и понимать их узкие места. Персоналу информационной безопасности требуется комбинированный набор технических и аналитических навыков, что, в свою очередь, изменит учебные программы для подготовки специалистов по кибербезопасности.

Таким образом, обеспечение и регулирование информационной безопасности России с каждым годом совершенствуется и пополняется новыми компаниями-разработчиками и компаниями-интегральщиками. Из-за пандемии в 2020 году произошел заметный скачок в количестве и качестве инструментов обеспечения безопасности, так как большая часть организаций перешла на удаленный режим работы и возникла необходимость в защите и шифровании важной информации.

2.3 Зарубежный опыт обеспечения информационной безопасности

Различными способами ведущие страны достаточно эффективно реализуют национальную политику информационной безопасности[28]. Самые современные и надежные системы защиты информации действуют в Соединенных Штатах Америки, Израиле, Германии, Великобритании и Китае. Таким образом, в тех странах, которые постоянно находятся под сильным внешним информационным влиянием и поэтому вынуждены создавать национальные системы защиты. Последние имеют достаточно активную составляющую, благодаря которой можно проводить информационные и психологические мероприятия и кибер-атаки против стран-противников.

Система информационной безопасности Соединенных Штатов Америки особенно эффективна. Ее система имеет достаточную широкую основу, которая охватывает все слои жизнедеятельность, из-за чего она довольно многомерна, в то же время подчинена единой верховенствующей стратегии.

Законодательство достаточно ответственно регулирует вопросы обеспечения безопасности информации в государственных компьютерных системах, борьбы с кибер-преступлениями, регулирования прав граждан на доступ к информации и тайны личной жизни[29]:

1. Закон «О компьютерной безопасности»;
2. Закон «О совершенствовании информационной безопасности»;
3. Закон «О компьютерном мошенничестве и злоупотреблениях»;
4. Закон «О злоупотреблении компьютерами»;
5. Закон «О свободе информации»;
6. Закон «Об освещении деятельности правительства»;
7. Закон «Об охране личных тайн».

Административно-организационная система обеспечения и реализации информационной безопасности в США направлена на координацию всех действий по защите информации и реализацию единой государственной политики. Президент

---

[28] Бекмурзаев И. Д. Цифровая экономика и четвертая промышленная революция: перспективы для бизнеса / И. Д. Бекмурзаев, Я. Э. Дадаев // Современные контуры цифровой экономики: материалы Междунар. науч - практ. конф. – Грозный, 2018. – С. 639-643.

[29] Бекмурзаев И. Д. Международный опыт обеспечения национальной информационной безопасности / И. Д. Бекмурзаев, А. Х. Курбанов, С. Д. Хажмурадова // Общество, экономика, управление. – 2020. – Т.5, №1. – С. 6-9.

Соединенных Штатов Америки является главным ответственным лицом за обеспечение и реализацию национальной информационной безопасности[30].

Другие европейские страны, имеющие достаточно высокий уровень жизни, также уделяют много внимания на развитие информационной безопасности, основываясь на собственной национальной политике и принципах о защите населения от неизбежных в современном информационном обществе угроз и опасностей.

Во Франции сфера обеспечения информационной безопасности вместе с информационным сектором является очень важной сферой жизни вместе с экономикой, политикой и культурой. Следовательно, информационная сфера имеет такой же высокий уровень защиты, как и другие сферы жизнедеятельности. Отсюда можно сделать вывод, что что именно здесь концепция современной многовекторной геостратегии французской правящей элиты отражает новый элемент, напрямую влияющий на оперативное принятие решений государственных или негосударственных организаций, СМИ, а также национальных специальных служб, которые участвуют в процессе внедрения и реализации стратегии. Таким образом, информационное пространство во Франции считается одним из приоритетных объектов защиты, обеспечиваемых всеми возможными законодательными, организационными, административными, властными и информационными технологиями.

Правительство Китайской Народной Республики в этом вопросе менее демократично, чем в США и Франции. В информационной политике КНР преобладают принципы внедрения достаточно моноцентрических, оборонительных и наступательных доктрин. Стратегия Китая в большинстве своем направлена на интеграцию в мировое сообщество сферы информационной безопасности, принимая политику, имеющую демократическую ориентацию как фактора модернизации политической системы КНР и ее потенциального лидерства на региональном и международном уровне. Проект под названием «Великая китайская информационная стена» на данный момент принят и действует в Китае, который направлен на фильтрацию всех информации, проходящей по техническим каналам и социальным сетям страны. Таким образом, Китайская Народная Республика демонстрирует относительно успешные результаты внутри своей стратегии, охватывая практический весь массив информации как внутри страны, так и направленной за рубеж. Учитывая, что у Китая своя собственная, ни на какие другие не похожая, модель стратегии, то страна постепенно добивается успеха, выполняя задачу по выходу на

[30] Бабаш А. В. История защиты информации в зарубежных странах: учебное пособие : [для студентов вузов по направлению информационной безопасности и прикладной информатики] / А. В. Бабаш, Д. А. Ларин. - Москва : РИОР : Инфра-М, 2013, 283 с.

лидирующие позиции среды крупных игроков мировой арены в сфере информационной безопасности, создавая себе конкуренцию даже в Соединенных Штатах Америки.

Вопросы защиты персональных данных, регулируемые во многих странах, заслуживают особого внимания в сфере правового обеспечения информационной безопасности. В Испании, например, в 1999 году был принят органический закон «О защите персональных данных», согласно которому ресурсы являются общедоступными: списки кандидатов, выдвинутых на эту должность, телефонные справочники (в соответствии с законом) и списки лиц профессии, которые содержат информацию об именах, званиях, профессии, занятии, ученой степени, адресе и обозначении принадлежности к этим группам, а также официальные публикации, бюллетени и средства массовой информации[31].

Если владелец персональных данных не является резидентом Евросоюза и использует средства, находящиеся в Испании для обработки персональных данных, он должен назначить представителя в Испании. В случае, если лицо не назначит представителя из Испании, то ему будут выдвинуты санкции, так как все операции с персональными данными, которые обрабатываются внутри принятой стратегии, могут быть использованы только с согласия субъекта.

Таким образом, в мире есть страны с разными традициями государственного управления, которые относительно эффективно реализуют национальную политику информационной безопасности различными способами: от создания систематизированной нормативной базы до использования различных материальных ресурсов. Изучая успешный опыт ведущих стран, можно получить выводы, которые положительно повлияли бы на решение многих проблем, существующих сегодня в сфере безопасности информационного пространства.

[31] Основы государственной политики Российской Федерации в области международной информационной безопасности на период до 2020 года : утв. указом Президента РФ от 22 апреля 2014 г. // КонсультантПлюс : справ. Правовая система. – Версия проф. – М., 2021. – Режим доступа : локальная сеть Науч. б-ки Том. гос. ун-та.

ЗАКЛЮЧЕНИЕ

Сфера информационной безопасности является одной из самых динамичных и развивающихся, что подразумевает под собой довольно обширную законодательную базу, которая несомненно развивается и подстраивается под все изменения в обществе. По этой причине учитываются все основные аспекты защиты информации, которые, в свою очередь, улучшаются. Необходимо учитывать основные категории информационной безопасности, известные с конца прошлого века, и совершенствовать их в поисках новых, менее затратных и более эффективных способов решения проблем.

Защита информации должна работать бесперебойно, постоянно приспосабливаясь к изменениям в системах, а также в их комплексе и взаимосвязи, чтобы улавливать все направления возможных угроз. Чтобы специалист добился наиболее стабильного и безопасного состояния организации на рынке, необходимо использовать все методы (физические средства защиты информации, базовые средства защиты электронной информации, резервное копирование данных, шифрование данных при передаче информации в электронном формате, анти-DDoS, план аварийного восстановления данных).

Таким образом, в дипломной работе в качестве теоретической основы были рассмотрены такие аспекты информационной безопасности как основные виды угроз и возможные способы их нивелирования, методологические указания по классификации и ранжированию угроз информационной безопасности государства, предприятий и личности, а также подробно рассмотрена сравнительная характеристика специфики организации обеспечения безопасности информации в государственных органах США, стран Европы, Азии и Российской Федерации. Исходя из результатов исследования можно сделать вывод, что российская система информационной безопасности все еще находится в стадии разработки и не отвечает всем требованиям, необходимым для обеспечения информационной безопасности международного уровня. Однако, изучение успешного опыта ведущих стран мира позволяет сделать выводы, которые положительно повлияют на решение многих проблем, существующих сегодня в области безопасности информационного пространства.

В качестве подробного исследования положительных и отрицательных сторон обеспечения информационной безопасности в Российской Федерации были изучены методологические и статистические данные для получения полной информации о состоянии кибербезопасности страны на данный период времени. Также, для

установления причинно-следственной связи процессов обеспечения и регулирования информационной безопасности в XXI веке необходимо рассмотреть и изучить истоки развития кибербезопасности в стране, что несомненно, показывает актуальность выбранной темы как в прошлом веке, так и на данный момент. Исходя из полученных данных, мы можем сделать вывод о том, что обеспечение и регулирование информационной безопасности в России ежегодно совершенствуется и дополняется новыми компаниями-разработчиками и интеграционными компаниями. В результате пандемии в 2020 году произошел значительный скачок в количестве и качестве инструментов безопасности, поскольку большинство организаций перешли на удаленную работу, и возникла потребность в защите и шифровании не только пользовательской, но и конфиденциальной информации.

В дипломной работе, также была рассмотрена конкретная государственная организация, один из структурных элементов которой занимается формированием и обеспечением информационной безопасности персональных данных Администрации Томской области. Для изучения данного вопроса была использована внутренняя политика обработки защищаемой информации, не содержащей государственную тайну и модель угроз безопасности персональных данных, которая была создана и адаптирована непосредственно под специфику Администрации. Исходя из полученных данных была рассчитана и составлена карта рисков, а также рассчитан возможный ущерб в случае утечки информации. На основе результатов исследования можно сделать вывод о том, что Администрация Томской области имеет исключительно репутационные риски при утечке персональных данных, однако, была рассчитана полная стоимость всех инструментов обеспечения информационной безопасности государственной организации по состоянию на май 2021 года.

Так как у Администрации не было ни одного громкого инцидента, связанного с утечкой персональных данных можно сделать вывод о том, что имеющихся инструментов обеспечения безопасности достаточно, однако, в качестве рекомендации можно сказать, что необходимо обновлять сертификаты и лицензии на инструменты обеспечения безопасности (антивирусные программы, средства защиты от несанкционированного доступа, средства криптографической защиты, средства доверенной загрузки средств вычислительной техники), а также следить за обновлениями в сфере инструментов и способов защиты информации, используя из них самые надежные.

В последние годы были предприняты определенные практические меры по усилению информационной безопасности в Российской Федерации. Началось более углубленное формирование нормативно-правового обеспечения информационной

безопасности - приняты законы «О безопасности» и «О государственной тайне», началась работа по созданию механизмов их реализации и подготовка законопроектов, регулирующих деятельность в сфере информационной безопасности.

ЛИТЕРАТУРА

1. Конституция Российской Федерации: принята всенародным голосованием 12.12.1993 с изменениями, одобренными в ходе общероссийского голосования 01.07.2020 от 14 марта 2020 г. N 1-ФКЗ) / Собрание законодательства Российской Федерации. – 2020. – Ст. 79.

2. Доктрина информационной безопасности Российской Федерации : утв. указом Президента от 5 декабря 2016 г. №646 // КонсультантПлюс : справ. Правовая система. – Версия проф. – М., 2021. – Режим доступа : локальная сеть Науч. б-ки Том. гос. ун-та.

3. Об информации, информационных технологиях и о защите информации Федеральный закон от 27 июля 2006 г. N 149-ФЗ // КонсультантПлюс : справ. Правовая система. – Версия проф. – М., 2021. – Режим доступа : локальная сеть Науч. б-ки Том. гос. ун-та.

4. О внесении изменений в Уголовный кодекс Российской Федерации и Уголовно-процессуальный кодекс Российской Федерации в части установления дополнительных мер противодействия терроризму и обеспечения общественной безопасности : Федеральный закон от 6 июля 2016 г. N 375-ФЗ // КонсультантПлюс : справ. Правовая система. – Версия проф. – М., 2021. – Режим доступа : локальная сеть Науч. б-ки Том. гос. ун-та.

5. Вопросы Федеральной службы по техническому и экспортному контролю : утв. указом Президента РФ от 16 августа 2004г. №1085 // КонсультантПлюс : справ. Правовая система. – Версия проф. – М., 2021. – Режим доступа : локальная сеть Науч. б-ки Том. гос. ун-та.

6. Вопросы Совета Безопасности Российской Федерации (вместе с «Положением о Межведомственной комиссии Совета Безопасности Российской Федерации по безопасности в экономической и социальной сфере», «Положением о Межведомственной комиссии Совета Безопасности Российской Федерации по военной безопасности», «Положением о Межведомственной комиссии Совета Безопасности Российской Федерации по информационной безопасности», «Положением о Межведомственной комиссии Совета Безопасности Российской Федерации по общественной безопасности», «Положением о Межведомственной комиссии Совета Безопасности Российской Федерации по проблемам Содружества Независимых Государств» : утв. указом Президента РФ от 06.05.2011 N 590 (ред. от 07.03.2020 // КонсультантПлюс : справ.

Правовая система. – Версия проф. – М., 2021. – Режим доступа : локальная сеть Науч. б-ки Том. гос. ун-та.

7. Об утверждении Основ государственной политики Российской Федерации в области международной информационной безопасности : утв. указом Президента РФ от 12 апреля 2021 №213 // КонсультантПлюс : справ. Правовая система. – Версия проф. – М., 2021. – Режим доступа : локальная сеть Науч. б-ки Том. гос. ун-та.

8. Основы государственной политики Российской Федерации в области международной информационной безопасности на период до 2020 года : утв. указом Президента РФ от 22 апреля 2014 г. // КонсультантПлюс : справ. Правовая система. – Версия проф. – М., 2021. – Режим доступа : локальная сеть Науч. б-ки Том. гос. ун-та.

9. Модель угроз безопасности персональных данных Федеральной государственной информационной системы «Единая информационная система управления кадровым составом государственной гражданской службы Российской Федерации» утверждена заместителем Губернатора Томской области по вопросам безопасности Администрации Томской области от 25.12.2020г. – 2020.

10. Политика в отношении обработки защищаемой информации, не содержащей сведения, составляющие государственную тайну, в Администрации Томской области утверждена заместителем Губернатора Томской области и начальником Департамента по профилактике коррупционных и иных правонарушений Администрации Томской области от 25.12.2020. – 2020.

11. Технический проект подсистемы обеспечения информационной безопасности ФГИС «ЕИСУ КС» утвержден заместителем Губернатора Томской области по вопросам безопасности Администрации Томской области от 25.12.2020г. – 2020.

12. Акопов Г. Л. Интернет и политика : модернизация политической системы на основе инновационных политических интернет-коммуникаций : монография / Г. Л. Акопов. - Москва : Кнорус, 2017. - 237, [1] с.: ил., табл.

13. Актуальные киберугрозы: итоги 2020 года. [Электронный ресурс] // Positive Technologies – [М.], 2021. - URL: https://www.ptsecurity.com/ru-ru/research/analytics/cybersecurity-threatscape-2020/ (Дата обращения 12.05.2021).

14. Алабина Ю. Ф. Технология построения VPN ViPNet : курс лекций / Ю. Ф. Алабина, А. О. Чефранова. - Москва : Горячая линия - Телеком, 2018. - 338 с.: ил., табл.

15. Аналитика. Российский рынок информационной безопасности [Электронный ресурс] // CNews. - URL: https://www.cnews.ru/reviews/security2019/articles/rossijskij_rynok_informatsionnoj (Дата обращения 26.04.2021).

16. Артамонова Я. С. Информационная безопасность российского общества: теоретические основания и практика политического обеспечения : автореферат диссертации на соискание ученой степени доктора политических наук : 23.00.02. - Москва : [б. и.], 2014. - 56 с.

17. Бабаш А. В. Информационная безопасность. История защиты информации в России [Текст] : [учебное пособие] / А. В. Бабаш, Е. К. Баранова, Д. А. Ларин. - Москва : КДУ, 2013. - 735 с.

18. Бабаш А. В. История защиты информации в зарубежных странах: учебное пособие : [для студентов вузов по направлению информационной безопасности и прикладной информатики] / А. В. Бабаш, Д. А. Ларин. - Москва : РИОР : Инфра-М, 2013, 283 с.

19. Балановская А. В. Анализ и тенденции рынка информационной безопасности в России / А. В. Балановская, А. В. Волкодаевая // Экономические науки. 2019. №1. С. 226-229.

20. Безопасность информационных систем. Понятия экономической и информационной безопасности // Национальный открытый университет. – М., 2021. – С. 1-2.

21. Бекмурзаев И. Д. Международный опыт обеспечения национальной информационной безопасности / И. Д. Бекмурзаев, А. Х. Курбанов, С. Д. Хажмурадова // Общество, экономика, управление. – 2020. – Т.5, №1. – С. 6-9.

22. Бекмурзаев И. Д. Цифровая экономика и четвертая промышленная революция: перспективы для бизнеса / И. Д. Бекмурзаев, Я. Э. Дадаев // Современные контуры цифровой экономики: материалы Междунар. науч - практ. конф. – Грозный, 2018. – С. 639-643.

23. Бирюков А. А. Информационная безопасность: защита и нападение. – 2-е изд., перераб. и доп. – Москва : ДМК Пресс, 2017. – 434 с.

24. Бузов Г. А. Выявление специальных технических средств несанкционированного получения информации. – М. : Горячая линия - Телеком, 2019. - 203 с.: ил., табл.

25. Бузов Г. А. Защита информации ограниченного доступа от утечки по техническим каналам / Г. А. Бузов. - Москва : Горячая линия - Телеком, 2019. - 585 с.

26. Володенков С. В. Интернет-коммуникации в глобальном пространстве современного политического управления / Моск. гос. ун-т им. М. В. Ломоносова, Фак. политологии. - Москва : Издательство Московского университета, 2015. – 269 с.

27. Ворона В. А. Теоретические основы обеспечения безопасности объектов информатизации : [учебное пособие для вузов] / В. А. Ворона, Л. В. Митрякова, Тихонов В. А. - Москва : Горячая линия - Телеком, 2016. - 303 с.

28. Горбатов В. С. Введение в информационную безопасность : [учебное пособие для студентов, обучающихся по направлениям подготовки (специальностям), не входящим в направление подготовки "Информационная безопасность"] / В. С. Горбатов, В. И. Королев, А. А. Малюк [и др.]. - Москва : Горячая линия - Телеком, 2014. - 288 с.: ил., табл.

29. Грунин О. А. Основы теории и практики экономической безопасности: Учеб. пособие / О. А. Грунин, С. О. Грунин; М-во образования Рос. Федерации. С.-Петерб. - СПб.: СПбГИЭУ, 2002, С. 90.

30. Еськов А. В. Защита информационных систем с содержанием персональных данных, эксплуатируемых в ОВД / А. В. Еськов, И. И. Кирюшин // Проблемы правоохранительной деятельности. 2015. № 2. С. 76-79.

31. Зарицкая А. С. Установление тождественной связи информационного и репутационного рисков в общей структуре рисков органов государственной власти / А. С. Зарицкая, В. С. Симанков. — Текст : непосредственный // Молодой ученый. — 2013. — № 12 (59). — С. 83-85.

32. Камский В. А. Защита личной информации в Интернете, смартфоне и компьютере / Камский В. А. - Санкт-Петербург : Наука и техника, 2017. - 272 с.

33. Канарский Д. С. Сигналы систем электрорадиосвязи : учебное пособие : [для студентов] / Д. С. Канарский, Н. С. Николаев. - Москва : Русайнс, 2021. – 158 с.

34. Кин Э. Ничего личного : как социальные сети, поисковые системы и спецслужбы используют наши персональные данные : пер. с англ. / Эндрю Кин ; [ред. В. Мылов]. - Москва : Альпина Паблишер, 2016. - 220 с.

35. Косовец А. А. Информационная безопасность в системе обеспечения экономической и национальной безопасности России // Вестник Академии экономической безопасности МВД России. Право. – 2011. - №2. – С. 20-22.

36. Лободина, А. С. Информационная безопасность / А. С. Лободина, В. В. Ермолаева. — Текст : непосредственный // Молодой ученый. — 2017. — № 17 (151). — С. 17-20.

37. Лопатин Ю.Н. Информационная безопасность в России. Проблемы, поиски решений // Информационная безопасность в России. 2018. №2. С. 51-52.

38. Марчев Д. В. Базовые криптографические алгоритмы защиты информации : учебное пособие : [для студентов высших учебных заведений] / Д. В. Марчев, А. Н. Пылькин, О. Г. Швечкова. - Москва : Курс, 2020. – 167 с.

39. Международные стандарты по оценке безопасности информационных технологий. Федеральные критерии безопасности информационных технологий // Справочник по информационной безопасности. – М., 2020. – 14 с.

40. Моделирование угроз информационной безопасности: различные подходы // Национальный открытый университет. – М., 2021. – С. 21-23.

41. Основы государственной политики РФ в области международной информационной безопасности [Электронный ресурс] // Varonis Systems. - URL: https://www.varonis.com/ru/ (Дата обращения 26.04.2021).

42. Понятия экономической и информационной безопасности // Открытая библиотека учебной информации. – М., 2021. – С. 13-15.

43. Проскурин В. Г. Защита в операционных системах : [учебное пособие для студентов] / Проскурин В. Г.. - Москва : Горячая линия - Телеком, 2016. - 192 с.: ил.

44. Рейтинг российских производителей средств защиты информации [Электронный ресурс] // CISO CLUB. Информационная безопасность. - URL: https://cisoclub.ru/ (Дата обращения 26.04.2021).

45. Родичев Ю. А. Нормативная база и стандарты в области информационной безопасности [Текст] : учебное пособие для студентов, обучающихся по программам высшего образования укрупненной группы специальностей и направлений подготовки «Информационной безопасность». - Санкт-Петербург [и др.] : Питер, 2017. - 254 с.

46. Савченко О. А. Специальные критерии информационной безопасности органа предварительного расследования // Вопросы кибербезопасности. 2016. №2 (15). С. 4-6.

47. Стрельцов А. А. Государственная информационная политика: основы теории / А. А. Стрельцов; под общ. ред. В. А. Садовничего, В. П. Шерстюка ; Московский гос. ун-т им. М. В. Ломоносова ; Координац. совет по приоритетному науч. направл. "Безопасность и противодействие терроризму". - Москва : Изд-во МЦНМО, 2010. - 107 с.

48. Угрозы информационной безопасности. Построение систем защиты от угрозы нарушения конфиденциальности информации. Защита информации от утечки по техническим каналам // Портал электронных систем обучения. – Екатеринбург., 2021. – С. 47-50.

49. Утечки информации ограниченного доступа: отчет за 9 месяцев 2020 года // Экспертно-аналитический центр InfoWatch. – М., 2020. – С. 9-13.

50. Яблоков Н. П. Криминалистическая методика расследования: история, современное состояние и проблемы: монография. М.: Норма, 2016. – 191 с.

51. Freedom in Europe : securing our technological future / European Commission. - Luxembourg : Publications Office of the European Union, 2010. - 18 p.

52. Mueller J.P. Security for Web Developers: Using javascript, HTML, and CSS / J.P. Mueller - O'Reilly Media, 2015 – 384 p.

53. National Institute of Standards and Technology [Электронный ресурс] – URL: https://www.nist.gov/ (Дата обращения 10.05.2021).

АНТИПЛАГИАТ
ОБНАРУЖЕНИЕ ЗАИМСТВОВАНИЙ

Отчет о проверке на заимствования №1

Автор: Плахова Анастасия Андреевна
Проверяющий: Шаринская Людмила Геннадьевна (s.scharinskaja@lib.tsu.ru / ID: 340)
Организация: Томский Государственный Университет

Отчет предоставлен сервисом «Антиплагиат» - http://tsu.antiplagiat.ru

ИНФОРМАЦИЯ О ДОКУМЕНТЕ

№ документа: 34
Начало загрузки: 14.06.2021 09:30:31
Длительность загрузки: 00:00:19
Корректировка от 14.06.2021 09:35:17
Имя исходного файла: ВКР Плахова А.А..pdf
Название документа: Информационная безопасность
Размер текста: 1 кБ
Тип документа: Выпускная квалификационная работа
Символов в тексте: 151129
Слов в тексте: 17063
Число предложений: 787

ИНФОРМАЦИЯ ОБ ОТЧЕТЕ

Последний готовый отчет (ред.)
Начало проверки: 14.06.2021 09:30:52
Длительность проверки: 00:00:40
Комментарии: [Автосохраненная версия]
Поиск с учетом редактирования: да
Модули поиска: ИПС Адилет, Библиография, Сводная коллекция ЭБС, Интернет Плюс, Сводная коллекция РГБ, Цитирование, Переводные заимствования (RuEn), Переводные заимствования по eLIBRARY.RU (EnRu), Переводные заимствования по Интернету (EnRu), Переводные заимствования издательства Wiley (RuEn), eLIBRARY.RU, СПС ГАРАНТ, Медицина, Диссертации НББ, Перефразирования по eLIBRARY.RU, Перефразирования по Интернету, Патенты СССР, РФ, СНГ, СМИ России и СНГ, Шаблонные фразы, Модуль поиска "ТГУ", Кольцо вузов, Издательство Wiley, Переводные заимствования

ЗАИМСТВОВАНИЯ	САМОЦИТИРОВАНИЯ	ЦИТИРОВАНИЯ	ОРИГИНАЛЬНОСТЬ
20,49%	0%	7,07%	72,44%

Заимствования — доля всех найденных текстовых пересечений, за исключением тех, которые система отнесла к цитированиям, по отношению к общему объему документа.
Самоцитирования — доля фрагментов текста проверяемого документа, совпадающий или почти совпадающий с фрагментом текста источника, автором или соавтором которого является автор проверяемого документа, по отношению к общему объему документа.
Цитирования — доля текстовых пересечений, которые не являются авторскими, но система посчитала их использование корректным, по отношению к общему объему документа. Сюда относятся оформленные по ГОСТу цитаты; общеупотребительные выражения; фрагменты текста, найденные в источниках из коллекций нормативно-правовой документации.
Текстовое пересечение — фрагмент текста проверяемого документа, совпадающий или почти совпадающий с фрагментом текста источника.
Источник — документ, проиндексированный в системе и содержащийся в модуле поиска, по которому проводится проверка.
Оригинальность — доля фрагментов текста проверяемого документа, не обнаруженных ни в одном источнике, по которым шла проверка, по отношению к общему объему документа.
Заимствования, самоцитирования, цитирования и оригинальность являются отдельными показателями и в сумме дают 100%, что соответствует всему тексту проверяемого документа.
Обращаем Ваше внимание, что система находит текстовые пересечения проверяемого документа с проиндексированными в системе текстовыми источниками. При этом система является вспомогательным инструментом, определение корректности и правомерности заимствований или цитирований, а также авторства текстовых фрагментов проверяемого документа остается в компетенции проверяющего.

№	Доля в отчете	Источник	Актуален на	Модуль поиска	Комментарии
[01]	0,87%	http://alapaevskoe.ru/uploads/document/6974/%5Balfadok%5D-model-ugroz-bezopasnosti-pdn---buhgalterskij-uchet.docx http://alapaevskoe.ru	09 Ноя 2020	Интернет Плюс	
[02]	1,41%	Модель угроз безопасности персональных данных (стр. 3) | Авторская платформа Pandia.ru https://pandia.ru	09 Ноя 2020	Интернет Плюс	
[03]	0,63%	НИР_РАНХиГС_Госзадание_2018_тема_18.19	12 Фев 2019	Кольцо вузов	
[04]	0%	Приказ Министерства внутренней политики, информации и связи Республики Крым от 17 октября 2017 г. N 297 "Об утверждении политики в отношении обработки защищаемой информации" http://ivo.garant.ru	21 Фев 2019	СПС ГАРАНТ	
[05]	1,05%	ОРГАНИЗАЦИОННОЕ И ПРАВОВОЕ ОБЕСПЕЧЕНИЕ ИНФОРМАЦИОННОЙ БЕЗОПАСНОСТИ. Учебник и практикум для бакалавриата и магистратуры.pdf	22 Фев 2017	Сводная коллекция ЭБС	
[06]	1,19%	Кураленко, Алексей Игоревич Методика аудита информационной безопасности информационно-телекоммуникационной системы : диссертация ... кандидата технических наук : 05.13.19 Томск 2015 http://dlib.rsl.ru	27 Дек 2019	Сводная коллекция РГБ	
[07]	0,5%	Пояснительная записка	13 Июн 2017	Кольцо вузов	
[08]	0%	Приказ Департамента здравоохранения Курганской области от 30 мая 2018 г. N 632 "Об утверждении перечня угроз безопасности персональных данных, актуальных при обработке персональных данных в информационных системах персональных данных в Департаменте здра... http://ivo.garant.ru	14 Авг 2018	СПС ГАРАНТ	
[09]	0,15%	Политика в отношении обработки защищаемой информации, не содержащей сведения, составляющие государственную тайну, в ООО «НПЦ «КСБ» - АльфаДок https://alfa-doc.ru	05 Июн 2019	Интернет Плюс	
[10]	0,09%	КЗ.zip/Иванов СИ.docx	30 Окт 2013	Кольцо вузов	
[11]	0,27%	Политика в отношении обработки защищаемой информации, не содержащей сведения, составляющие государственную тайну	10 Дек 2017	Интернет Плюс	

Рецензия

на дипломную работу по теме:

«Информационная безопасность: оценка состояния, инструменты управления и способы обеспечения (на примере информационных систем Администрации Томской области»,

выполненную студентом (студенткой)

ИЭМ ТГУ

Плаховой Анастасией Андреевной

Дипломная работа «Информационная безопасность: оценка состояния, инструменты управления и способы обеспечения (на примере информационных систем Администрации Томской области» выполнена в соответствии с заданием научного руководителя в полном объеме.

Тема дипломной работы является актуальной, так как в условиях интенсивной цифровизации всех без исключения сфер жизнедеятельности общества проблема обеспечения защиты информации выдвигается на первый план, придавая информационной безопасности статус базисной. Значимость информационной составляющей в функционировании субъекта любого уровня позволяет рассматривать ее как инструмент конкурентоспособности, провоцирующий нелегитимную деятельность отдельных участников общественных отношений по получению определённых сведений и использованию их, и, соответственно, мотивирующий субъекта к разработке и реализации совокупности мер по недопущению этого. Тем самым проблема информационной безопасности приобретает высокую научную и практическую значимость.

Целью работы явилась оценка состояния информационной безопасности, а также исследование инструментов управления и возможных способов ее обеспечения на основе данных Администрации Томской области.

Работа состоит из введения, трех глав, заключения, списка литературы.

Первая глава посвящена исследованию теоретических основ формирования и обеспечения информационной безопасности, рассмотрена роль последней, определены угрозы и указана специфика организации информационной безопасности в органах государственного управления. Во второй главе рассмотрено состояние информационной безопасности в Российской Федерации с акцентированием внимания на отечественном и зарубежном опыте. Глава 3 связана с оценкой организации функционирования информационных систем Администрации Томской области с позиции ее обеспечения, моделирования спектра возможных угроз, оценки ущерба в случае утечки информации.

В работе можно выделить следующие достоинства - глубокая теоретическая проработка с последующей систематизацией данных, подкрепленная фактологическим материалом.

В работе использован необходимый объём нормативных и литературных источников. Содержание дипломной работы соответствует названию. Тема раскрыта в достаточном объеме. Работа является законченным исследованием, выполнена грамотно, аккуратно, соответствует всем требованиям, предъявляемым к дипломным работам.

Автор показал умение изучать и обобщать литературные и интернет источники, делать выводы и предположения. В процессе работы использован необходимый объем нормативных, литературных и интернет источников.

Таким образом, считаю, что дипломная работа Плаховой А.А. может быть допущена к защите и заслуживает оценки *отлично*, а автор присвоения квалификации "Экономист" по специальности 38.05.01 – Экономическая безопасность.

Рецензент:

Председатель Комитета обеспечения
информационной безопасности
Администрации Томской области

П.И.Маляр
03.06.2021

Отзыв

на дипломную работу по теме:
«Информационная безопасность: оценка состояния, инструменты управления и способы обеспечения (на примере информационных систем Администрации Томской области»,
выполненную студентом (студенткой) ИЭМ ТГУ
(специальность 38.05.01 – Экономическая безопасность)
Плаховой Анастасией Андреевной

Актуальность темы связана с приобретением информационным ресурсами статуса ключевого ресурса в организации функционирования субъекта национальной экономики. С одной стороны, это приводит к трансформации подходов к организации деятельности, возникновению новых. Более совершенных технологий взаимодействий, их наполненности, с другой – требует решения проблемы защищенности информации. Организация деятельности на основе построения, трансформации и эксплуатации информационных потоков обусловливает настоятельность формирования и непрерывного совершенствования подходов к обеспечению информационной безопасности.

Первая глава посвящена исследованию теоретических основ формирования и обеспечения информационной безопасности, рассмотрению угроз в данной сфере. Во второй главе приведена оценка отечественного и зарубежного опыта. Глава 3 связана с рассмотрением подходов к организации информационных систем Администрации Томской области.

В работе использован необходимый объём нормативных и литературных источников. Содержание ВКР соответствует её названию. Тема раскрыта в достаточном объеме. Работа является законченным исследованием, выполнена грамотно, аккуратно, соответствует всем требованиям, предъявляемым к ВКР.

Таким образом, считаю, что дипломная работа Плаховой А.А. может быть допущена к защите и заслуживает оценки «отлично», а автор присвоения квалификации «Экономист» по специальности 38.05.01 «Экономическая безопасность».

Научный руководитель
докт.экон.наук, профессор
НИ ТГУ

Матюгина Э.Г.

Руководителю ООП
канд. экон. наук, доценту
В. В. Копилевич
От студента 5 курса НИ ТГУ гр. 27609/1
А. А. Плаховой

В связи с использованием в выпускной квалификационной работе материалов, предназначенных для служебного пользования сотрудниками Администрации Томской области, прошу разрешить исключить из открытого доступа материалы главы 3 «Информационные системы Администрации Томской области», а также приложения к ВКР «Актуальные угрозы безопасности информации в Федеральной Государственной информационной системе «Единая информационная система управления кадровым составом» и «Определение актуальности угроз в Федеральной Государственной информационной системе «Единая информационная система управления кадровым составом» Администрации Томской области».

Руководитель ООП

Исключить из открытого доступа материалы гл. 3.

_____ / В. В. Копилевич
подпись инициалы, фамилия

_____ / А. А. Плахова
подпись инициалы, фамилия

«18» июня 2021 г.