МИНИСТЕРСТВО НАУКИ И ВЫСШЕГО ОБРАЗОВАНИЯ РФ
ФЕДЕРАЛЬНОЕ ГОСУДАРСТВЕННОЕ БЮДЖЕТНОЕ ОБРАЗОВАТЕЛЬНОЕ УЧРЕЖДЕНИЕ ВЫСШЕГО ОБРАЗОВАНИЯ
«ДОНСКОЙ ГОСУДАРСТВЕННЫЙ ТЕХНИЧЕСКИЙ УНИВЕРСИТЕТ»
(ДГТУ)

Факультет: Отдел магистратуры УПКВК
(наименование факультета)
Кафедра: Вычислительные системы и информационная безопасность
(наименование кафедры)

ПОЯСНИТЕЛЬНАЯ ЗАПИСКА

к контрольной работе по дисциплине (модулю): Социальные и философские проблемы ИТ-отрасли
(наименование учебной дисциплины (модуля))
на тему: Концепция организационного построения защищенной информационной системы торгового предприятия в аспекте социальных проблем
Автор работы: _____ Иванов И.И.
(подпись) (Ф.И.О)
Направление/специальность, профиль/специализация:
09.04.02 Информационные системы и технологии
(код направления) (наименование направления (специальности))
Профиль – Информационные системы в технологиях защиты информации
(наименование профиля (специализации))
Обозначение контрольной работы: вариант №1 Группа: МЗИС21
Руководитель работы: _____ доцент, Газизов А.Р.
(подпись) (должность, Ф.И.О)
Контрольная работа защищена: «30» декабря 2022 г. _____ _____
(дата) (оценка) (подпись)

Ростов-на-Дону
2022

МИНИСТЕРСТВО НАУКИ И ВЫСШЕГО ОБРАЗОВАНИЯ РФ
ФЕДЕРАЛЬНОЕ ГОСУДАРСТВЕННОЕ БЮДЖЕТНОЕ ОБРАЗОВАТЕЛЬНОЕ УЧРЕЖДЕНИЕ ВЫСШЕГО ОБРАЗОВАНИЯ
«ДОНСКОЙ ГОСУДАРСТВЕННЫЙ ТЕХНИЧЕСКИЙ УНИВЕРСИТЕТ»
(ДГТУ)

Факультет Отдел магистратуры УПКВК
Кафедра Вычислительные системы и информационная безопасность

ЗАДАНИЕ

к контрольной работе по дисциплине (модулю): Социальные и философские проблемы ИТ-отрасли
(наименование учебной дисциплины (модуля))

Магистрант: Иванов И.И. Группа: МЗИС21

Обозначение контрольной работы: Вариант №1

Тема: Концепция организационного построения защищенной информационной системы торгового предприятия в аспекте социальных проблем

Срок представления работы к защите: «30» декабря 2022 г.

Исходные данные для контрольной работы – классификация информационных ресурсов торгового предприятия; принципы построения защищенной информационной системы торгового предприятия; требования к защищенной информационной системы торгового предприятия; рекомендации к построению защищенной информационной системы торгового предприятия; составляющие системы защиты информационной системы торгового предприятия; политика безопасности информационной системы торгового предприятия.

Содержание пояснительной записки:
ВВЕДЕНИЕ: актуальность контрольной работы
НАИМЕНОВАНИЕ И СОДЕРЖАНИЕ РАЗДЕЛОВ:
1. Классификация информационных ресурсов торгового предприятия
2. Принципы построения защищенной информационной системы торгового предприятия
3. Требования к защищенной информационной системы торгового предприятия
4. Рекомендации к построению защищенной информационной системы торгового предприятия
5. Составляющие системы защиты информационной системы торгового предприятия
6. Политика безопасности информационной системы торгового предприятия
ЗАКЛЮЧЕНИЕ: выводы
Перечень использованных информационных ресуросов

Руководитель работы: _____«01» сентября 2022 г. Газизов А.Р.
(подпись, дата) (Ф.И.О.)

Задание принял к исполнению: _____«01» сентября 2022 г. Иванов И.И.
(подпись, дата) (Ф.И.О.)

СОДЕРЖАНИЕ

Введение 5
1 Классификация информационных ресурсов торгового предприятия 6
2 Принципы построения защищенной информационной системы торгового предприятия 10
3 Требования к защищенной информационной системы торгового предприятия 12
5 Составляющие системы защиты информационной системы торгового предприятия 15
6 Политика безопасности информационной системы торгового предприятия 19
Заключение 20
Перечень использованных информационных ресурсов 21

Введение

В соответствии с национальным стандартом РФ «ГОСТ Р 51303-2013. Торговля. Термины и определения», торговое предприятие (ТП) – это имущественный комплекс, расположенный в торговом объекте, а также вне торгового объекта, используемый торговыми организациями или индивидуальными предпринимателями для осуществления продажи товаров и оказания услуг торговли. Информационные ресурсы ТП – это совокупность всей получаемой и накапливаемой информации в процессе практической деятельности работников предприятия и функционирования специальных устройств, используемых в управлении ТП. Информация ТП – это данные, извлекаемые из деловой документации предприятия, по вопросам продажи товаров и оказания услуг торговли и получаемые от партнеров в порядке информационного взаимодействия, т. е. процесса передачи-приема информации, при обеспечении возможности сбора, обработки, продуцирования, архивирования, транслирования информации средствами информационных и коммуникационных технологий (ИКТ). В ТП основными источниками информации являются люди, т. е. работники предприятия, а также электронные и бумажные носители информации. При этом количество электронных и бумажных носителей информации в процессе информационного взаимодействия между пользователями присутствует в равных пропорциях.

1 Классификация информационных ресурсов торгового предприятия

Применение бумажных носителей информации усложняет операции по ее сбору, продуцированию, накоплению, хранению, обработке и передаче, однако делает ее менее уязвимой для злоумышленника. С учетом недостаточного внедрения программно-аппаратных средств защиты информации в средства ИКТ ТП (электронная цифровая подпись (ЭЦП), межсетевой экран и пр.) в процессе информационного взаимодействия пользователей, а также необходимости документального оформления торговых операций, присутствие бумажных носителей информации является актуальным до настоящего времени. С учетом специфики продажи товаров и оказания услуг торговли информационные ресурсы ТП подлежат следующей классификации:

1) Информация о клиентах. Данная информация хранится в базе данных (БД) информационной системы (ИС) ТП. Это данные о физических или юридических лицах, ведущих сотрудничество с ТП. Доступ к информации о клиентах ограничен. Конфиденциальность информации о клиентах обусловлена тем, что намеренное ее искажение или утрата может привести к негативным последствиям, в частности, к потере прибыли предприятием. При этом под ИС ТП, функционирующей на базе средств ИКТ, будем понимать систему передачи и приема информации ТП, состоящую из источника информации, передатчика, канала связи, приемника информации и источника помех [2, 3].

2) Информация о работниках. Данная информация включает персональные данные каждого работника, в том числе паспортные данные, сведения о месте проживания, семейном положении, предыдущем месте работы и пр. Личные персональные данные каждый работник предоставляет в кадровый отдел ТП при поступлении на работу, давая письменное согласие на их обработку; персональные данные вносятся в личное дело работника, далее упорядочиваются и хранятся в кадровом отделе

предприятия. В соответствии с Федеральным законом от 27.07.2006 № 152-ФЗ (в ред. от 21.07.2014 г.) «О персональных данных» [4] данная информация является конфиденциальной, а доступ к ней имеют исключительно работники кадрового органа, а также лица, имеющие на это полномочия в соответствии с должностной инструкцией. Основными носителями информации о работниках ТП являются бумажные. Совокупность данных о работниках ТП в ИС, т. е. БД, включающая ключевые сведения о работниках, подлежит защите с помощью программно-аппаратных средств.

3) Коммуникативная информация. Данная информация обеспечивает информационное взаимодействие работников ТП и внешних контрагентов. Она находится в свободном доступе (как правило, на сайте ТП), включает сведения о форме собственности и наименовании ТП, фактический и юридический адреса, контактную информацию и пр.; эта информация не подлежит защите.

4) Общая информация. Это стандартные показатели, характеризующие деятельность ТП, без учета его специфики; она находится в свободном доступе и не подлежит защите.

5) Финансовая информация. Данная информация является весьма ценной для злоумышленника с коммерческой точки зрения, что предполагает ее надежную защиту. Она включает сведения о счетах предприятия, его финансовых операциях, финансовых активах, заработной плате работников и пр., т. е. полностью описывает финансовое состояние ТП в данный момент или конкретный период времени. Нарушение целостности, конфиденциальности и доступности финансовой информации может привести к катастрофическим последствиям для ТП, поэтому не стоит пренебрегать ее защитой.

Таблица – Степени важности информационных ресурсов торгового предприятия

Вид информации	Степень важности	Проявление угрозы
Юридическая	Высокая	Весьма значительные (критичные) финансовые потери торгового предприятия. Потеря репутации, приведшая к существенному снижению коммерческой и деловой активности торгового предприятия. Дезорганизация деятельности торгового предприятия на длительный период времени.
Финансовая	Высокая	
Информация о клиентах	Высокая	
Информация о работниках	Средняя	Значительные (некритичные) финансовые потери торгового предприятия. Потеря репутации, которая может вызвать уменьшение потока заказов и негативную реакцию деловых партнеров. Повышенное внимание государственных органов (в том числе фискальных, правоохранительных, контролирующих), как следствие – снижение деловой активности торгового предприятия.
Коммуникативная	Низкая	Незначительные финансовые потери торгового предприятия. Необходимость восстановления информационных ресурсов торгового предприятия.
Общая	Низкая	

Основная часть финансовой информации хранится в цифровой форме и обрабатывается с помощью специального программного обеспечения (ПО), что делает ее наиболее уязвимой и доступной извне для злоумышленников, поэтому в процессе информационного взаимодействия пользователей ТП необходимо уделять повышенное внимание защите финансовой информации (ЗИ).

6) Юридическая информация. Данная информация является общедоступной и может разглашаться без каких-либо отрицательных последствий для ТП. Она включает: устав предприятия; приказы, регламентирующие работу предприятия; меморандумы (соглашения) о сотрудничестве с внешними контрагентами, т. е. коммерческими и некоммерческими организациями и пр. Таким образом, данные документы являются юридической надстройкой ТП и регулируют внутренние и внешние правоотношения предприятия. Юридическая информация хранится, как правило, на бумажных носителях; вместе с тем с постепенным внедрением систем электронного документооборота многие

документы издаются в цифровой форме и подписываются с помощью ЭЦП, т. е. аналога подписи физического лица, полученного с использованием средств ИКТ и криптографического преобразования информации. По истечении установленного срока хранения юридические документы сдаются на хранение в архив.

Вышеупомянутые виды информации обладают различной степенью значимости для ТП, следовательно, имеют различную степень коммерческой и иной ценности для злоумышленника (табл.).

2 Принципы построения защищенной информационной системы торгового предприятия

На основе анализа возможностей средств ИКТ в качестве средств обработки информации в ИС ТП при ведении делопроизводства и средств автоматизации принятия управленческих решений, а также анализа степени важности информационных ресурсов ТП, построение защищенной ИС ТП должно базироваться на следующих принципах:

1) Принцип непрерывности. Является первым и наиболее важным. Суть этого принципа заключается в постоянном контроле защищенности ИС; выявлении слабых мест ИС, а также потенциально возможных каналов утечки информации и несанкционированного доступа к системе; обновлении и дополнении механизмов защиты в зависимости от изменения характера внутренних и внешних угроз ИС; обосновании и реализации на этой основе наиболее рациональных методов, способов и путей ЗИ.

2) Принцип комплексности. Исходит из характера действий злоумышленников, стремящихся любыми способами добыть важную информацию для конкурентной борьбы. В данном принципе правомерно утверждение, что оружие защиты должно быть адекватно оружию нападения.

3) Принцип системности. Наибольший эффект достигается в случае, когда все используемые средства, методы и мероприятия объединяются в единый, целостный механизм, т. е. систему защиты ИС. В этом случае проявляются системные свойства защиты ИС, не присущие отдельным элементам, а также возможность управления защитой ИС и перераспределения ресурсов ЗИ для обеспечения непрерывного функционирования системы.

4) Принцип законности, разумной достаточности и профессионализма работников ТП. Важнейшими условиями обеспечения безопасности являются законность, достаточность, соблюдение баланса интересов личности и предприятия, высокий профессионализм работников,

занимающихся вопросами защиты ИС, а также подготовка пользователей и соблюдение ими установленных правил ЗИ, взаимная ответственность руководителей и специалистов предприятия; информационное взаимодействие с государственными и правоохранительными органами.

3 Требования к защищенной информационной системы торгового предприятия

Выделенные принципы позволяют определить тематическое наполнение требований к защищенной ИС ТП [6]:

1) Централизованность. Процесс управления ИС всегда централизован, поэтому структура системы, реализующей процесс ее защиты, должна соответствовать структуре самой ИС.

2) Плановость. Процесс планирования осуществляется для организации информационного взаимодействия всех структурных единиц ТП в интересах реализации принятой политики защиты ИС; каждая служба, отдел, направление разрабатывают детальные планы ЗИ в сфере своей компетенции и с учетом общей цели предприятия.

3) Конкретность и целенаправленность. Защите подлежат конкретные ИР, которые могут представлять интерес для потенциальных конкурентов.

4) Активность, т. е. обеспечивать ЗИ необходимо с достаточной степенью настойчивости и целеустремленности. Это требование предполагает наличие в составе системы защиты ИС средств прогнозирования, экспертных систем и других инструментариев, позволяющих реализовать наряду с принципом «обнаружить и устранить» принцип «предвидеть и предотвратить».

5) Надежность и универсальность: охват всего комплекса информационной деятельности ТП; методы и средства защиты ИС должны надежно перекрывать все возможные каналы утечки информации и противодействовать способам несанкционированного доступа независимо от формы представления информации, языка ее выражения, а также вида носителя, на котором она закреплена

6) Нестандартность в сравнении с ИС других предприятий и разнообразие по используемым средствам и методам защиты.

7) Открытость для изменения и дополнения мер обеспечения

защиты ИС.

8) Экономическая эффективность, т. е. затраты на формирование защищенной

ИС не должны превышать размеров возможного ущерба.

4 Рекомендации к построению защищенной информационной системы торгового предприятия

Наряду с принципами и требованиями существуют рекомендации, которые следует применять при построении защищенной ИС ТП:

– «механизмы» защиты ИС должны быть просты для технического обслуживания и «прозрачны» для пользователей;

– каждый пользователь должен иметь минимальный набор «привилегий», необходимых для информационного взаимодействия;

– возможность отключения «механизмов» защиты ИС в «особых» случаях, когда механизмы «мешают» информационному взаимодействию пользователей;

– независимость «механизмов» защиты ИС от самой системы; разработчики «механизмов» защиты ИС должны предполагать, что пользователи имеют наихудшие намерения или будут совершать серьезные ошибки и искать пути обхода механизмов защиты ИС;

– отсутствие на ТП излишней информации о существовании «механизмов» защиты ИС.

5 Составляющие системы защиты информационной системы торгового предприятия

Система защиты ИС ТП должна включать две составляющие: организационно-распорядительную и техническую.

1) Организационно-распорядительная составляющая. В её основе лежит комплекс внутренних документов, регламентирующих вопросы обеспечения защиты ИС:

− документы стратегического (первого) уровня политики ЗИ, определяющие стратегические цели руководства ТП в данной области;

− документы второго уровня политики ЗИ, включающие организационно-распорядительные документы, регламентирующие вопросы организации и проведения работ по защите ИС;

− документы третьего уровня политики ЗИ, включающие исполнительную документацию, должностные обязанности и инструкции, а также эксплуатационные документы средств защиты ИС, в том числе документы, регламентирующие вопросы ЗИ.

Организационно-распорядительная составляющая при построении защищенной ИС ТП должна включать мероприятия, выполняемые в процессе создания и функционирования ИС в целях обеспечения ЗИ. Эти мероприятия охватывают все составляющие структуры ИС, а также элементы ее защиты на всех этапах жизненного цикла.

Деятельность по реализации организационных мероприятий при построении защищенной ИС ТП опирается на нормативную базу по ЗИ и должна включать:

− ограничение физического доступа к элементам ИС и реализацию мер по обеспечению режима конфиденциальности;

− ограничение возможности перехвата информации из ИС посредством электромагнитного излучения и наводок;

− ограничение доступа к ресурсам ИС посредством разграничения доступа, применения методов криптографии при передаче данных,

выявления и уничтожения закладных устройств;

– создание резервных (в том числе бумажных) копий «критичной» информации;

борьбу с компьютерными вирусами;

– организацию и поддержание пропускного режима, контроля посетителей, охраны помещений и территории;

– организацию защиты информации в ИС, в том числе назначение ответственного за ЗИ на предприятии, проведение систематического мониторинга деятельности персонала, соблюдение порядка и правил учета, хранения и уничтожения документов.

Деятельность по реализации организационных мероприятий при взаимодействии с работниками ТП должна включать:

– собеседование при приеме на работу;

– ознакомление работника с регламентом работы в ИС;

– обучение работника правилам работы в ИС;

– инструктаж о необходимости сохранения коммерческой тайны при увольнении с работы.

Ознакомление работника с регламентом работы в ИС ТП, а также его обучение правилам работы в системе предполагают формирование компетенций, т. е. знаний и умений, а также компетентности, т. е. практических навыков работы в ИС (в том числе относительно работы с информацией, представляющей коммерческую тайну предприятия).

Инструктаж работника о необходимости сохранения коммерческой тайны при его увольнении с работы необходим для предотвращения ее разглашения.

2) Техническая составляющая. Она должна включать:

– подсистему антивирусной защиты, которая должна соответствовать следующим требованиям: организация мониторинга антивирусной активности, организация двухуровневой антивирусной защиты с применением антивирусных приложений различных

производителей, обеспечение антивирусной защиты серверного оборудования;

− подсистему резервного копирования и архивирования, которая должна соответствовать следующим требованиям: формирование соответствующих документов и инструкций (регламентирующих процесс резервного копирования и архивирования и связанных с производственной необходимостью), организация резервного копирования для всех серверов (указанных в регламентах резервного копирования), разработка процедур, регулярное проведение и тестирование резервных копий;

− подсистему защиты электронной почты, которая должна соответствовать следующим требованиям: задействование механизмов защищенного почтового обмена внутри ИС; обеспечение аутентификации пользователей при отправке электронной почты;

− подсистему обнаружения атак; в целях контроля и оперативного реагирования на выполнение несанкционированных операций в сегменте сопряжения и серверных сегментах ИС рекомендуется внедрить систему обнаружения атак, предназначенную для своевременного обнаружения атак на узлы ИС;

− подсистему защиты каналов передачи данных, что позволит значительно увеличить безопасность информационного взаимодействия внешних контрагентов и работников ТП;

− подсистему идентификации и аутентификации пользователей для централизации управления аутентификационной информацией и обеспечения соответствия ИС требованиям нормативных документов Федеральной службы по техническому и экспортному контролю (ФСТЭК) РФ.

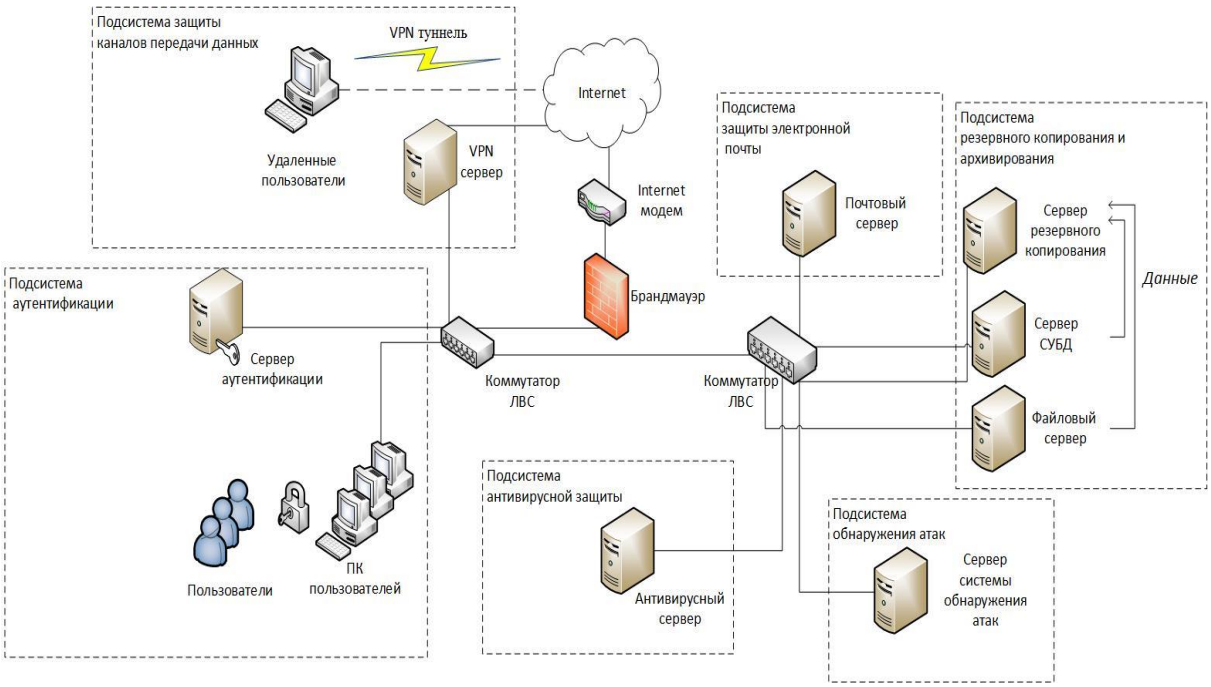

Рисунок – Модули защищенной ИС ТП

Построение защищенной ИС ТП предполагает ее модернизацию в будущем, при этом необходимо поэтапное создание и внедрение взаимосвязанных модулей (функциональных подсистем), обеспечивающих ее защиту. Модули защищенной ИС ТП представлены на рисунке.

6 Политика безопасности информационной системы торгового предприятия

Политика безопасности ИС ТП – организованная совокупность средств, методов и мероприятий по информационной безопасности, нацеленная на обеспечение целостности, конфиденциальности и доступности ИР предприятия.

Политика безопасности – один из ключевых компонентов общей программы защиты ИС ТП. Политика безопасности является тем «заявлением» руководства ТП, в котором могут быть сформулированы изначальные требования относительно защиты ИС. Целесообразно описать цели защиты ИС ТП, обязанности и т. п. в отдельной политике, которую нужно использовать совместно с существующей общей политикой безопасности.

Политика безопасности ИС ТП должна устанавливать:

− значение информации, т. е. определять позицию руководства предприятия по вопросу ценности информации в ИС;

− ответственность, т. е. устанавливать работников предприятия, ответственных за ЗИ в ИС;

− обязательства предприятия по ЗИ в ИС;

− область применения, т. е. сегменты ИС предприятия, на которые распространяется действие политики.

Политика безопасности ИС ТП после ее утверждения не должна подвергаться корректировке. Например, включение в политику требования использовать определенный пакет для обнаружения вирусов, включающего название пакета, может быть слишком конкретным с точки зрения темпа разработки антивирусных программ. Более корректным будет обозначить, что ПО обнаружения вирусов должно находиться на ПЭВМ пользователей ИС, серверах и пр., что позволит администраторам ИС самим определять конкретный вид антивирусного ПО.

Заключение

Модульный принцип построения защищенной ИС ТП сделает систему более гибкой, а также позволит заменить или модернизировать каждую функциональную подсистему, не затрагивая остальные модули ИС.

Представленная концепция построения ИС ТП является универсальной, она позволит обеспечить защищенное информационное взаимодействие в аспекте функционирования ИС при осуществлении деятельности в процессе передачи-приема информации, при реализации обратной связи, развитых средств ведения интерактивного диалога при обеспечении возможности сбора, обработки, продуцирования, архивирования, передачи, транслирования информации в рамках ТП.

Перечень использованных информационных ресурсов

1. Geekkies: сайт. – 2022. – URL. https://geekkies.in.ua/crossplatform/chto-takoe-virtualbox-i-kak-ej-polzovatsja.html (дата обращения: 05.07.2022).

2. RU-center: сайт. – 2022. – URL. https://www.nic.ru/help/bazy-dannyh-1228/ (дата обращения: 05.07.2022).

3. Академик – информационная безопасность: сайт. – URL. https://dic.academic.ru/dic.nsf/dic_economic_law/5569/ИНФОРМАЦИОННАЯ (дата обращения: 05.07.2022).

4. Академик – официальная терминология: сайт. – 2022. – URL. https://official.academic.ru/7175 (дата обращения: 05.07.2022).

5. Академик – словарь чрезвычайных ситуаций: сайт. – 2022. – URL. https://dic.academic.ru/dic.nsf/emergency/777/ (дата обращения: 05.07.2022).

6. Астайкин, А. И. Методы и средства обеспечения программно-аппаратной защиты информации: научно-техническое издание / А. И. Астайкин, А. П. Мартынов, Д. Б. Николаев, В. Н. Фомченко. – Саров: Российский федеральный ядерный центр – ВНИИЭФ, 2015. – 224 с. – ISBN 978-5-9515-0305-3. – Текст: электронный // Цифровой образовательный ресурс IPR SMART: [сайт]. – URL: https://www.iprbookshop.ru/60959.html (дата обращения: 05.07.2022). – Режим доступа: для авторизир. пользователей.

7. Башлы, П. Н. Информационная безопасность и защита информации: учебник / П. Н. Башлы, А. В. Бабаш, Е. К. Баранова. – Москва: РИОР, 2013. – 222 с. – ISBN 978-5-369-01178-2. – Текст: электронный. – URL: https://znanium.com/catalog/product/405000 (дата обращения: 05.07.2022). – Режим доступа: по подписке.

8. Википедия – Kali Linux: сайт. – URL. https://ru.wikipedia.org/wiki/Kali_Linux (дата обращения: 05.07.2022).

9. Гатчин, Ю. А. Основы информационной безопасности: учебное пособие / Ю. А. Гатчин, Е. В. Климова. – Санкт-Петербург: Университет ИТМО, 2009. – 84 с. – Текст: электронный // Цифровой образовательный ресурс IPR SMART: [сайт]. – URL: https://www.iprbookshop.ru/67463.html (дата обращения: 05.07.2022). – Режим доступа: для авторизир. пользователей.

10. Голембиовская, О. М. Этапы формирования модели угроз и модели нарушителя информационной безопасности с учетом изменений законодательства Российской Федерации: учебное пособие / О. М. Голембиовская, М. Ю. Рытов, К. Е. Шинаков [и др.]. – Саратов: Вузовское образование, 2021. – 265 с. – ISBN 978-5-4487-0791-9. – Текст: электронный // Цифровой образовательный ресурс IPR SMART: [сайт]. – URL: https://www.iprbookshop.ru/109162.html (дата обращения: 05.07.2022). – Режим доступа: для авторизир. пользователей.

11. Громов, Ю. Ю. Программно-аппаратные средства защиты информационных систем : учебное пособие / Ю. Ю. Громов, О. Г. Иванова, К. В. Стародубов, А. А. Кадыков. – Тамбов: Тамбовский государственный технический университет, ЭБС АСВ, 2017. – 193 с. – ISBN 978-5-8265-1737-6. – Текст: электронный // Цифровой образовательный ресурс IPR SMART: [сайт]. – URL: https://www.iprbookshop.ru/85968.html (дата обращения: 05.07.2022). – Режим доступа: для авторизир. пользователей.

12. Консультант плюс – Федеральный закон «Об информации, информационных технологиях и о защите информации» от 27.07.2006 N 149-ФЗ: сайт. – URL. http://www.consultant.ru/document/cons_doc_LAW_61798/ (дата обращения: 05.07.2022).

13. Основные проблемы защиты информации в сетях: сайт. – 2022. – URL. https://zen.yandex.com/media/id/5da8242eaad43600b1f1f9ed/osnovnye-

problemy-zascity-informacii-v-setiah-5da82678c31e4900ae31ec07 (дата обращения: 05.07.2022).

14. Правительство России – Постановление Правительства РФ от 01.11.2012 № 1119 «Об утверждении требований к защите персональных данных при их обработке в информационных системах персональных данных»: сайт. – URL. http://government.ru/docs/all/84743/ (дата обращения: 05.07.2022).

15. Ревнивых, А.В. Информационная безопасность в организациях: учебное пособие / А. В. Ревнивых. – Москва: Ай Пи Ар Медиа, 2021. – 83 с. – ISBN 978-5-4497-1164-9. – Текст: электронный // Цифровой образовательный ресурс IPR SMART: [сайт]. – URL: https://www.iprbookshop.ru/108227.html (дата обращения: 08.05.2022). – Режим доступа: для авторизир. пользователей.

16. Скабцов, Н. Аудит безопасности информационных систем. / Н. Скабцов. – СПб.: Питер, 2018. — 272 с.: ил. — (Серия «Библиотека программиста»).

17. ФСТЭК России – Приказ ФСТЭК России от 18 февраля 2013 г. №21 «Об утверждении состава и содержания организационных и технических мер по обеспечению безопасности персональных данных, при их обработке в информационных системах персональных данных»: сайт. – URL. https://fstec.ru/normotvorcheskaya/akty/53-prikazy/691-prikaz-fstek-rossii-ot-18-fevralya-2013-g-n-21 (дата обращения: 05.07.2022).

18. ФСТЭК России – Федеральный закон «О персональных данных» от 27.07.2006 N 152-ФЗ»: сайт. – URL. https://fstec.ru/tekhnicheskaya-zashchita-informatsii/dokumenty/107-zakony/365-federalnyj-zakon-ot-27-iyulya-2006-g-n-152-fz?highlight=WyIxNTItXHUwNDQ0XHUwNDM3Il0= (дата обращения: 05.07.2022).

19. Шаньгин, В. Ф. Информационная безопасность и защита информации / В. Ф. Шаньгин. – 2-е изд. – Саратов: Профобразование, 2019. – 702 с. – ISBN 978-5-4488-0070-2. – Текст: электронный // Цифровой

образовательный ресурс IPR SMART: [сайт]. – URL: https://www.iprbookshop.ru/87995.html (дата обращения: 05.07.2022). – Режим доступа: для авторизир. пользователей.

20. Шаньгин, В. Ф. Комплексная защита информации в корпоративных системах: учебное пособие / В. Ф. Шаньгин. – Москва: ФОРУМ: ИНФРА-М, 2020. – 592 с. – ISBN 978-5-8199-0730-6. – Текст: непосредственный.