МИНИСТЕРСТВО ПРОСВЕЩЕНИЯ РОССИЙСКОЙ ФЕДЕРАЦИИ
Федеральное государственное бюджетное Образовательное учреждение
высшего образования
«ЮЖНО-УРАЛЬСКИЙ ГОСУДАРСТВЕННЫЙ ГУМАНИТАРНО-ПЕДАГОГИЧЕСКИЙ УНИВЕРСИТЕТ» (ФГБОУ ВО «ЮУрГГПУ»)

ПРОФЕССИОНАЛЬНО-ПЕДАГОГИЧЕСКИЙ ИНСТИТУТ (ППИ)
КАФЕДРА АВТОМОБИЛЬНОГО ТРАНСПОРТА, ИНФОРМАЦИОННЫХ ТЕХНОЛОГИЙ И МЕТОДИКИ ОБУЧЕНИЯ ТЕХНИЧЕСКИМ ДИСЦИПЛИНАМ

Выбор средств защиты корпоративной информационной системы образовательной организации

Выпускная квалификационная работа по направлению
44.04.04 Профессиональное обучение (по отраслям)
Направленность программы магистратуры
«Управление информационной безопасностью в профессиональном образовании»
Форма обучения очная

Проверка на объем заимствований:
78,27 % авторского текста

Работа рекомендована/не рекомендована к защите
«13» 05 2023 г.
Зав. кафедрой АТИТ и МОТД
_____Руднев В.В.

Выполнил:
Студентка группы ОФ-209-210-2-1
Казанцева Мария Владимировна

Научный руководитель:
к.п.н, доцент кафедры АТ, ИТ и МОТД ППИ
Гафарова Елена Аркадьевна

Челябинск – 2023

СОДЕРЖАНИЕ

ВВЕДЕНИЕ..... 3
ГЛАВА 1. ТЕОРЕТИЧЕСКИЕ ОСНОВЫ ОРГАНИЗАЦИИ СИСТЕМЫ ЗАЩИТЫ КОРПОРАТИВНОЙ ИНФОРМАЦИОННОЙ СИСТЕМЫ ОБРАЗОВАТЕЛЬНОЙ ОРГАНИЗАЦИИ..... 9
1.1 Научно-методические основы корпоративной информационной системы и значение её защиты в образовательной организации..... 9
1.2 Нормативно-правовые требования к выбору средств защиты корпоративной информационной системы образовательной организации.... 14
1.3 Виды средств защиты корпоративной информационной системы образовательной организации..... 18
Вывод по первой главе 28
ГЛАВА 2. РАЗРАБОТКА РЕКОМЕНДАЦИЙ ПО ВЫБОРУ СРЕДСТВ ЗАЩИТЫ КОРПОРАТИВНОЙ ИНФОРМАЦИОННОЙ СИСТЕМЫ ОБРАЗОВАТЕЛЬНОЙ ОРГАНИЗАЦИИ..... 30
2.1 Анализ защиты корпоративной информационной системы образовательной организации ГБПОУ «Южно-Уральский государственный технический колледж»..... 30
2.2 Разработка рекомендаций по выбору средств защиты корпоративной информационной системы образовательной организации ГБПОУ «Южно-Уральский государственный технический колледж»..... 44
2.3 Разработка обучающего курса по применению средств защиты корпоративной информационной системы образовательной организации.... 65
2.4 Оценка эффективности рекомендаций по выбору средств защиты корпоративной информационной системы образовательной организации ГБПОУ «Южно-Уральский государственный технический колледж»..... 76
Вывод по второй главе..... 83
ЗАКЛЮЧЕНИЕ..... 86
СПИСОК ИСПОЛЬЗУЕМОЙ ЛИТЕРАТУРЫ..... 90

ВВЕДЕНИЕ

Одним из наиболее значимых классов информационных систем, подлежащих защите, выступают корпоративные информационные системы. От их успешного функционирования во многом зависит эффективность образовательных организаций, так как данные системы предназначены для автоматизации всего комплекса управленческих задач образовательной организации, а именно: сбор и анализ информации, планирование, организация и координация действий, контроль над исполнением, внутренняя и внешняя коммуникация и т.д. С помощью корпоративной информационной системы возможны: быстрый доступ ко всем необходимым данным в понятном для руководителя формате, упрощение процесса регистрации, хранения и обработки информации, формирование единого информационного пространства, уменьшение финансовых и трудовых затрат на организацию процессов планирования, управления и учёта деятельности организации.

Корпоративная информационная система образовательной организации является иерархически организованной распределённой информационной системой, охватывающей все подразделения образовательной организации и управления образовательным процессом, объединяющей их информационные ресурсы и обеспечивающей возможность оперативного взаимодействия.

Вопросом защиты корпоративной информационной системы образовательной организации занимались такие исследователи, как Г.В. Бабенко, Н.А. Гайдамакин, П.Н. Девянин, Д.П. Зегжда, П.Д. Зегжда, М. Лангехейнрих, М. Метцгер, Л. Хоффман, М. Шмит.

Существенный вклад в развитие и решение вопросов безопасности информационных систем внесли Р.М. Юсупов, В.И. Воробьёв, И.В. Котенко, А.А. Молдовян, Н.А. Молдовян, В.Ю. Осипов, И.Б. Саенко и другие.

В соответствии с п. 6 Постановления Правительства РФ «Об утверждении требований к защите персональных данных при их обработке в информационных системах персональных данных» актуальными угрозами

безопасности персональных данных понимается совокупность условий и факторов, создающих актуальную опасность несанкционированного, в том числе, случайного доступа к персональным данным при их обработке в информационной системе, результатом которого могут стать уничтожение, изменение, блокирование, копирование, предоставление, распространение персональных данных [32].

Существуют следующие группы источников угроз информационной безопасности:

1. Обусловленные действиями субъекта, которые могут привести к нарушению безопасности информации как умышленно (преднамеренно), так и случайно (непреднамеренно). В данном случае информация может быть похищена путём копирования на временные носители, переправлена по электронной почте, а при наличии доступа к серверу базы данных данные могут быть внесены вручную.

2. Обусловленные техническими средствами, где для хищения используются специальные программы, которые обеспечивают копирование паролей, копирование и перехват информации, внесение изменений в работу других программ. Здесь же могут быть использованы специальные технические средства и перехваты электромагнитного излучения.

3. Стихийные источники – обстоятельства, составляющие непреодолимую силу.

В соответствии с Приказом ФСТЭК России «Об утверждении требований о защите информации, не составляющей государственную тайну, содержащейся в государственных информационных системах» в информационной системе объектами защиты являются информация, содержащаяся в информационной системе, технические средства, общесистемное, прикладное, специальное программное обеспечение, информационные технологии, а также средства защиты информации [33].

Для обеспечения защиты корпоративной информационной системы образовательной организации от источников угроз необходимо применять

средства защиты, прошедших оценку соответствия в форме обязательной сертификации на соответствие требованиям по безопасности информации. В том числе защита должна производиться комплексно, то есть должно быть разграничение и контроль доступа к ресурсам, регистрация и анализ протекающих процессов, событий, пользователей, предотвращение возможных разрушительных воздействий на ресурсы и т.д.

Анализ текущего состояния защиты корпоративных информационных систем в образовательных организациях показывает, что средства защиты во многом не удовлетворяют требованиям практики.

Постоянное расширение функциональности корпоративных информационных систем, нарастание зависимости от информационной инфраструктуры и угроза уничтожения, изменения, блокирования, копирования, предоставления, распространения информации посредством несанкционированного доступа требует усиленной защиты этой системы за счёт выбора комплексных средств защиты.

Специфика защиты корпоративных информационных систем в образовательных организациях состоит в том, что в них содержится большой массив персональных данных, подлежащих защите. При этом обработка, хранение и передача их должна осуществляться в строгом соответствии с нормативными регулятивами.

Таким образом, существует **противоречие:** между потребностью применения комплексных средств защиты корпоративных информационных систем и неполнотой имеющихся рекомендаций по выбору средств защиты в связи со специфическими информационными процедурами в таких системах.

В связи с этим тема нашего исследования является актуальной: Выбор средств защиты корпоративной информационной системы образовательной организации.

Целью исследования является обоснование и разработка рекомендаций по выбору средств защиты корпоративной информационной системы образовательной организации.

Объект исследования: защита корпоративной информационной системы образовательной организации.

Предмет исследования: средства защиты корпоративной информационной системы образовательной организации.

Гипотеза исследования состоит в предположении о том, что эффективность защиты корпоративной информационной системы образовательной организации повысится при соблюдении рекомендаций по выбору средств защиты, разработанных на основе анализа модели угроз в образовательной организации.

В соответствии с целью, объектом и предметом исследования были поставлены следующие *задачи исследования*:

1) изучить научно-методические основы корпоративной информационной системы и значение её защиты в образовательной организации;

2) изучить нормативно-правовые требования к выбору средств защиты корпоративной информационной системы образовательной организации;

3) выявить виды средств защиты корпоративной информационной системы образовательной организации;

4) проанализировать состояние системы защиты корпоративной информационной системы образовательной организации;

5) разработать рекомендации по выбору средств защиты корпоративной информационной системы образовательной организации;

6) разработать обучающий курс по применению средств защиты корпоративной информационной системы образовательной организации;

7) оценить эффективность разработанных рекомендации по выбору средств защиты корпоративной информационной системы образовательной организации.

Методологическую основу исследования составили процессный и системный подходы, законодательные и нормативно-правовые документы РФ, метод сравнения и аналогии, методы оценки экономической эффективности.

Научная новизна исследования состоит в том, что сформулированы предложения по изменению действующих процессов в корпоративной информационной системе образовательной организации путем выбора средств защиты, обеспечивающих способность системы противостоять актуальным угрозам и атакам.

Практическая значимость исследования заключается в разработке рекомендаций по выбору средств защиты корпоративной информационной системы образовательной организации ГБПОУ СПО «ЮУрГТК», разработанных на основе анализа модели угроз названной организации, которые могут быть адаптированы для иной ОО СПО; разработке обучающего курса для системных администраторов по работе с межсетевым экраном UserGate.

База исследования: Государственное профессиональное образовательное учреждение «Южно-Уральский государственный технический колледж» (Политехнический комплекс).

Апробация исследования: Казанцева М. В. Выбор средств защиты корпоративной информационной системы образовательной организации / М. В. Казанцева // Молодежная политика и социальная миссия образования в эпоху глобализации и цифровизации : Материалы Международной Научно-практической конференции и молодежного форума, Челябинск, 06–08 апреля 2022 года. – Челябинск: ЗАО Библиотека А. Миллера, 2022. – С. 471-477; Казанцева М. В. Организация защиты корпоративной информационной системы в образовательной организации / М. В. Казанцева // Инновации в науке и практике : Сборник трудов по материалам XIII Всероссийского конкурса научно-исследовательских работ (12 июня 2023 г., г. Уфа). / – Уфа: Изд. НИЦ Вестник науки, 2023 – в печати; Казанцева М. В. Разработка обучающего курса для подготовки специалистов в сфере информационной

безопасности / М. В. Казанцева // Актуальные вопросы современной науки и инноватики : Сборник научных статей по материалам II Международной научно-практической конференции (16 июня 2023 г., г. Уфа) / – Уфа: Изд. НИЦ Вестник науки, 2023. – в печати.

Структура магистерской диссертации состоит из введения, двух глав, выводов к главам, заключения, библиографического списка.

ГЛАВА 1. ТЕОРЕТИЧЕСКИЕ ОСНОВЫ ОРГАНИЗАЦИИ СИСТЕМЫ ЗАЩИТЫ КОРПОРАТИВНОЙ ИНФОРМАЦИОННОЙ СИСТЕМЫ ОБРАЗОВАТЕЛЬНОЙ ОРГАНИЗАЦИИ

1.1 Научно-методические основы корпоративной информационной системы и значение её защиты в образовательной организации

На сегодняшний день деятельность образовательной организации рассматривается как взаимосвязанные, последовательные процессы, которые проходят через все подразделения, задействованы во всех службах и ориентированы на реализацию поставленных стратегических целей и задач. Полноценное функционирование современной образовательной организации уже немыслимо без единой корпоративной информационной системы, так как без использования технических автоматизированных средств поддержки уже невозможно обрабатывать большие объёмы информации.

Законодательно применение информационной системы в образовании регламентируется статьей 98 Федерального закона «Об образовании в РФ» от 29.12.2012 г. № 273-ФЗ [ФЗ 273].

Использованию информационных систем в процессе управления образовательной организацией отводится значительная роль. Рассмотрение данного вопроса представлено в фундаментальных трудах специалистов-практиков по использованию компьютерных программ в управленческой деятельности образовательной организации (Н. Н. Федякова [45], С. А. Шехматов [48], Т. Ш. Шихнабиева [49], И. Ю. Юханова [50], А. М. Ямалетдинова [51], А. И. Яценко [52]).

Понятийно информационная система представляет собой взаимосвязанную совокупность средств, методов и персонала, используемых для хранения, обработки и выдачи информации в интересах достижения поставленной цели. Она включает в себя вычислительное и коммуникационное оборудование, программное обеспечение, лингвистические средства и информационные ресурсы, а также системный

персонал, обеспечивающий поддержку динамической и информационной модели некоторой части реального мира для удовлетворения информационных потребностей.

Удачно дополнил данное определение исследователь А.А. Забуга, сфокусировав внимание на функциональных особенностях информационной системы, которая «позволяет упорядочить и координировать информацию, так как это необходимо для управляющего субъекта [14]. Суть её заключается в создании информационного контура вместе со средствами сбора, передачи, обработки и хранения информации».

Под понятием «корпоративная информационная система» мы будем понимать открытую интегрированную систему реального времени, автоматизирующую бизнес-процессы предприятия всех уровней и направлений деятельности, в том числе бизнес-процессы принятия управленческих решений. Она вводит комплексную автоматизацию образовательной организации, объединяя все структурные подразделения в единое информационное целое в условиях электронной информационно-образовательной среды. Подтверждение находим в работе исследователей А.Г. Додонова и Е.В. Флейтмана, которые определяют корпоративную информационную систему как «пронизывающую все составляющие, которые определяют функционирование корпорации» [13].

Основная задача и цель корпоративной информационной системы в процессе управления заключается в обеспечении взаимодействия всех структурных подразделений образовательной организации, в создании единого образовательного пространства. Она облегчает и упрощает выполнение рутинных операций, обеспечивает качественный сбор, хранение, обработку информации для эффективного принятия управленческих решений, формирует единую информационную структуру образовательной организации, организовывает информационное взаимодействие между сотрудниками всех подразделений и уровней.

Корпоративная информационная система отвечает всем функциям менеджмента и целевым установкам [47]:

– Мотивационно-целевая функция: информационная система позволяет вести базу данных о персональных достижениях сотрудников для стимулирования и повышения мотивации к профессиональному развитию; формирует электронное портфолио достижений; оформляет поощрения и взыскания; обеспечивает доступ к стратегическим и тактическим целям образовательной организации и персональным целям в контексте целей корпоративных.

– Информационно-аналитическая функция: собирает и анализирует информацию о текущих задачах, ставит новые задачи для оперативного информирования и исполнения поручений.

– Планово-прогностическая функция: контролирует расходы по выполняемым задачам, разрабатывает план мероприятий для исключения задвоенности и пересечений, планирует штатное расписание; планирует объёмы педагогической нагрузки.

– Организационно-исполнительная функция: выстраивает информацию в упорядоченную структуру, организовывает информационные потоки, распределяет информацию, что способствует эффективному принятию управленческих решений; распределяет задачи для рациональной организации труда преподавательского состава; ведёт электронный документооборот на уровне администрации образовательной организации.

– Контрольно-диагностическая функция: ведёт отчёты по обучающимся, табели посещаемости занятий для автоматизированного формирования ежемесячной и годовой отчётности.

– Регулятивно-коррекционная функция: позволяет оперативно вносить и получать обратную информацию об успеваемости обучающихся и др.

Таким образом корпоративная информационная система образовательной организации выступает одним из наиболее значимых классов информационных систем, подлежащих защите.

Информационная безопасность образовательной организации представляет собой комплекс мер различного характера, направленных на реализацию двух основных целей. Первой целью является защита персональных данных и информационного пространства от несанкционированных вмешательств, хищения информации и изменения конфигурации системы со стороны третьих лиц. Вторая цель информационной безопасности – защита обучающихся от любых видов пропаганды и рекламы, запрещенной законом информации [43].

Спектр интересов субъектов, связанных с использованием корпоративных информационных систем, можно разделить на следующие категории: обеспечение *доступности, целостности* и *конфиденциальности* информационных ресурсов и поддерживающей инфраструктуры [3].

Доступность – это возможность за приемлемое время получить требуемую информационную услугу.

Под *целостностью* подразумевается актуальность и непротиворечивость информации, ее защищенность от разрушения и несанкционированного изменения.

Конфиденциальность – это защита от несанкционированного доступа к информации. Источниками конфиденциальной информации в корпоративных информационных системах являются люди, документы, публикации, технические носители, технические средства обработки информации, продукция, промышленные и производственные отходы.

Защита информационных систем, обрабатывающих конфиденциальную информацию организации – это необходимость, благодаря которой можно существенно снизить риск утечки важных сведений. Она поможет грамотно и правильно организовать процесс обработки, хранения и передачи конфиденциальных сведений, находящихся в информационной системе.

Защита корпоративной информационной системы в образовательной организации имеет большое значение, так как она обеспечивает:

1. Конфиденциальность информации. Позволяет сохранить конфиденциальность персональных данных учеников и сотрудников, а также другой важной информации.

2. Непрерывность работы системы. Позволяет обеспечить непрерывность работы системы, что важно для эффективного функционирования образовательного процесса.

3. Защиту от вредоносных программ. Позволяет защитить систему от вирусов и других вредоносных программ, которые могут привести к потере данных и неполадкам в работе системы.

4. Управление доступом к информации. Позволяет определить уровень доступа каждого пользователя в зависимости от его должности и функций.

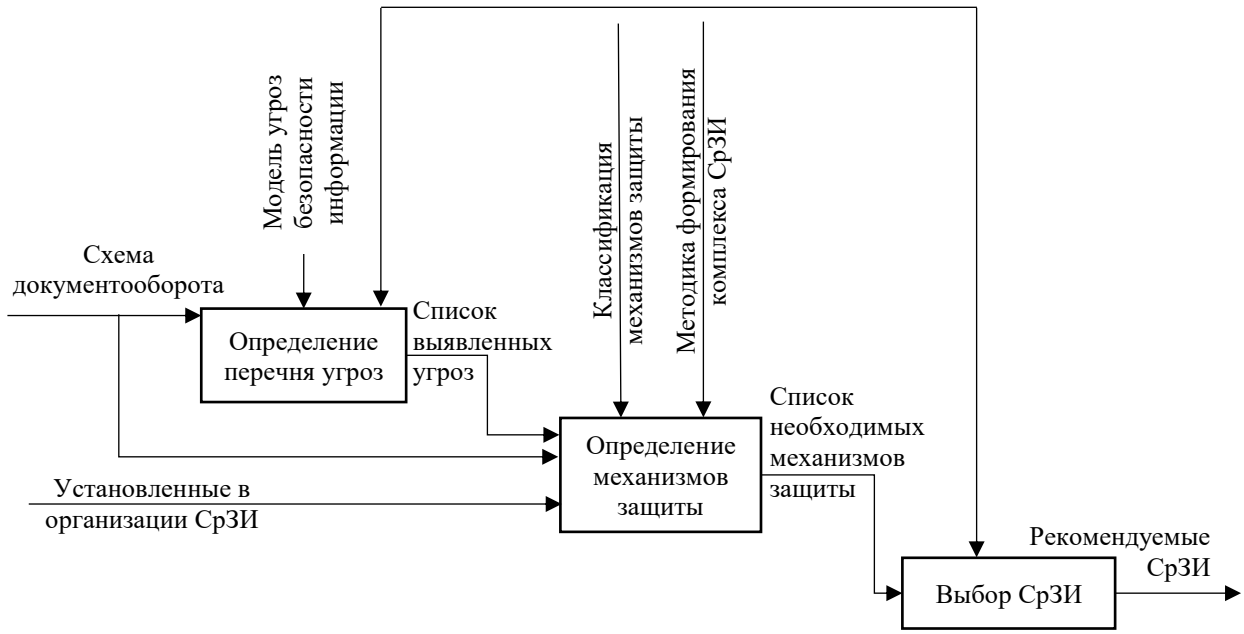
5. Сохранность данных. Позволяет сохранить данные в надежном месте и обеспечить их восстановление в случае потери.

Для защиты корпоративной информационной системы необходимо (рисунок 1):

– определить перечень угроз для каждого существующего в организации информационного потока;

– определить для каждого существующего информационного потока функционирующих в организации механизмов защиты и их достаточности;

– выбрать для существующего информационного потока надёжные средства защиты информации, позволяющие нейтрализовать «незакрытые» угрозы [15].



СрЗИ – средства защиты информации

Рисунок 1 – Декомпозиция методики формирования рекомендуемых средств защиты информации

Следовательно, использование средств защиты корпоративной информационной системы – необходимая мера, ведь именно благодаря им можно быть уверенным в безопасности данных образовательной организации.

1.2 Нормативно-правовые требования к выбору средств защиты корпоративной информационной системы образовательной организации

С учетом усиления роли информации на современном этапе, правовое регулирование общественных отношений, возникающих в информационной сфере, является приоритетным направлением в Российской Федерации, целью которого является обеспечение информационной безопасности [28]. Для управления образовательной организацией разнообразные корпоративные информационные системы используются достаточно давно и эффективно. Согласно статье 98 Федерального закона «Об образовании в Российской Федерации» от 29.12.2012 № 273-ФЗ в целях информационного обеспечения управления в системе образования уполномоченными органами

государственной власти Российской Федерации и органами государственной власти субъектов Российской Федерации создаются, формируются и ведутся информационные системы [34]. Данные информационные системы используются для предоставления услуг, с обеспечением конфиденциальности и безопасности содержащихся в них персональных данных. Информационная безопасность образовательных организаций отличается от других предприятий и организаций. Это обусловлено, прежде всего, специфическим характером угроз, а также публичной деятельностью образовательных организаций, которые вынуждены делать доступ к информационным ресурсам легким с целью удобства для граждан, что раскрывается в статье 29 Федерального закона «Об образовании в Российской Федерации» от 29.12.2012 № 273-ФЗ [34]. Поэтому вопрос организации защиты корпоративных информационных систем является в достаточной степени актуальным и диктует свои нормативно-правовые требования.

Федеральный закон «Об информации, информационных технологиях и о защите информации» от 27.07.2006 № 149-ФЗ регулирует отношения, возникающие при осуществлении права на поиск, получение, передачу, производство и распространение информации; применении информационных технологий; обеспечении защиты информации [29]. В силу того, что образовательные организации в своей деятельности неизбежно сталкиваются с информацией в различных формах её представления, действие данного ФЗ распространяется и на них.

В статье 5 Федерального закона «Об информации, информационных технологиях и о защите информации» говорится о том, что информация, в зависимости от категории доступа к ней, подразделяется на общедоступную информацию, а также на информацию, доступ к которой ограничен федеральными законами [29]. Согласно статье 7 Федерального закона «О персональных данных» от 27.07.2006 № 152-ФЗ к информации ограниченного доступа относятся персональные данные [27]. В главе 1 статье 3 данного закона вводится основное понятие: «Персональные данные – любая

информация, относящаяся к прямо или косвенно определенному или определяемому физическому лицу (субъекту персональных данных), в т.ч. его фамилия, имя, отчество, год, месяц, дата и место рождения, адрес, семейное, социальное, имущественное положение, образование, профессия, доходы, другая информация».

Отношения, связанные с обработкой персональных данных, осуществляемой федеральными органами государственной власти, органами государственной власти субъектов Российской Федерации, иными государственными органами, органами местного самоуправления, иными муниципальными органами, юридическими лицами и физическими лицами с использованием средств автоматизации, в том числе в информационно-телекоммуникационных сетях, или без использования таких средств, регламентируются Федеральным законом «О персональных данных» от 27.07.2006 N 152-ФЗ [27].

Согласно главе 1 статье 3 все образовательные организации являются операторами персональных данных, так как при организации образовательного процесса сталкиваются с обработкой информации, в том числе и в первую очередь с обработкой персональных данных.

Согласно главе 4 статье 19 оператор при обработке персональных данных обязан принимать необходимые правовые, организационные и технические меры или обеспечивать их принятие для защиты персональных данных от неправомерного или случайного доступа к ним, уничтожения, изменения, блокирования, копирования, предоставления, распространения персональных данных, а также от иных неправомерных действий в отношении персональных данных.

К правовым относятся меры, связанные с исполнением Федеральных законов и соблюдением Конституции РФ. К организационным относятся меры, связанные с разработкой, введением в эксплуатацию и соблюдением локальных организационных распорядительных документов организации. Техническими мерами обеспечения информационной безопасности являются

программные, программно-аппаратные, аппаратные и технические средства защиты информации.

Обеспечение безопасности персональных данных достигается за счёт определения угроз, применения средств защиты информации, прошедших процедуру оценки соответствия, оценки эффективности применяемых средств до ввода в эксплуатацию информационной системы [8].

С учетом возможного вреда субъекту персональных данных, объема и содержания обрабатываемых персональных данных, вида деятельности, при осуществлении которого обрабатываются персональные данные, актуальности угроз безопасности персональных данных устанавливаются уровни защищённости персональных данных при их обработке в информационных системах и требования к защите персональных данных при их обработке в информационных системах.

Уровни защищенности и требования к защите персональных данных закреплены в Постановлении Правительства РФ от 01.11.2012 № 1119 «Об утверждении требований к защите персональных данных при их обработке в информационных системах персональных данных» [32]. При обработке персональных данных в информационных системах устанавливаются 4 уровня защищенности персональных данных. Выбор уровня защищённости обуславливается актуальными угрозами информационной безопасности для определенной информационной системы персональных данных. Определение актуальных угроз является обязанностью оператора и производится самостоятельно, либо с привлечением специалистов.

После определения актуальных угроз и установления уровня защищенности производится выбор средств защиты информации в соответствии с нормативными правовыми актами, принятыми Федеральной службой безопасности Российской Федерации и Федеральной службой по техническому и экспортному контролю во исполнение части 4 статьи 19 Федерального закона «О персональных данных».

К данным документам относятся:

– Руководящий документ ФСТЭК России «Автоматизированные системы. Защита от несанкционированного доступа к информации. Классификация автоматизированных систем и требования по защите информации» от 30.03.1992 г., в котором устанавливается классификация автоматизированных систем, подлежащих защите от несанкционированного доступа к информации и требования по защите информации в автоматизированных системах различных классов [1].

– Руководящий документ Гостехкомиссии России «Средства вычислительной техники. Межсетевые экраны. Защита от несанкционированного доступа к информации. Показатели защищенности от несанкционированного доступа к информации» от 25.07.1997 г, в котором устанавливается классификация межсетевых экраном по уровню защищенности от несанкционированного доступа к информации на базе перечня показателей защищённости и совокупности описывающих требований [41].

1.3 Виды средств защиты корпоративной информационной системы образовательной организации

Противодействие многочисленным угрозам информационной безопасности предусматривает комплексное использование различных способов и мероприятий *организационного*, *правового*, *инженерно-технического, программно-аппаратного*, *криптографического* характера и т. п.

Организационные мероприятия по защите включают в себя совокупность действий по подбору и проверке персонала, участвующего в подготовке и эксплуатации программ и информации, строгое регламентирование процесса разработки и функционирования компьютерных систем [19].

К *правовым* мерам и средствам защиты относятся действующие в стране законы, нормативные акты, регламентирующие правила обращения с информацией и ответственность за их нарушение.

Инженерно-технические средства защиты достаточно многообразны и включают в себя физико-технические, аппаратные, технологические, программные, криптографические и другие средства. Данные средства обеспечивают следующие рубежи защиты: контролируемая территория, здание, помещение, отдельные устройства вместе с носителями информации.

Программно-аппаратные средства защиты непосредственно применяются в компьютерах и компьютерных сетях, содержат различные встраиваемые в компьютерную сеть электронные, электромеханические устройства. Специальные пакеты программ или отдельные программы реализуют такие функции защиты, как разграничение и контроль доступа к ресурсам, регистрация и анализ протекающих процессов, событий, пользователей, предотвращение возможных разрушительных воздействий на ресурсы и другие [20].

Общая структура комплексной системы защиты информации КИС представлена на рисунке 2.

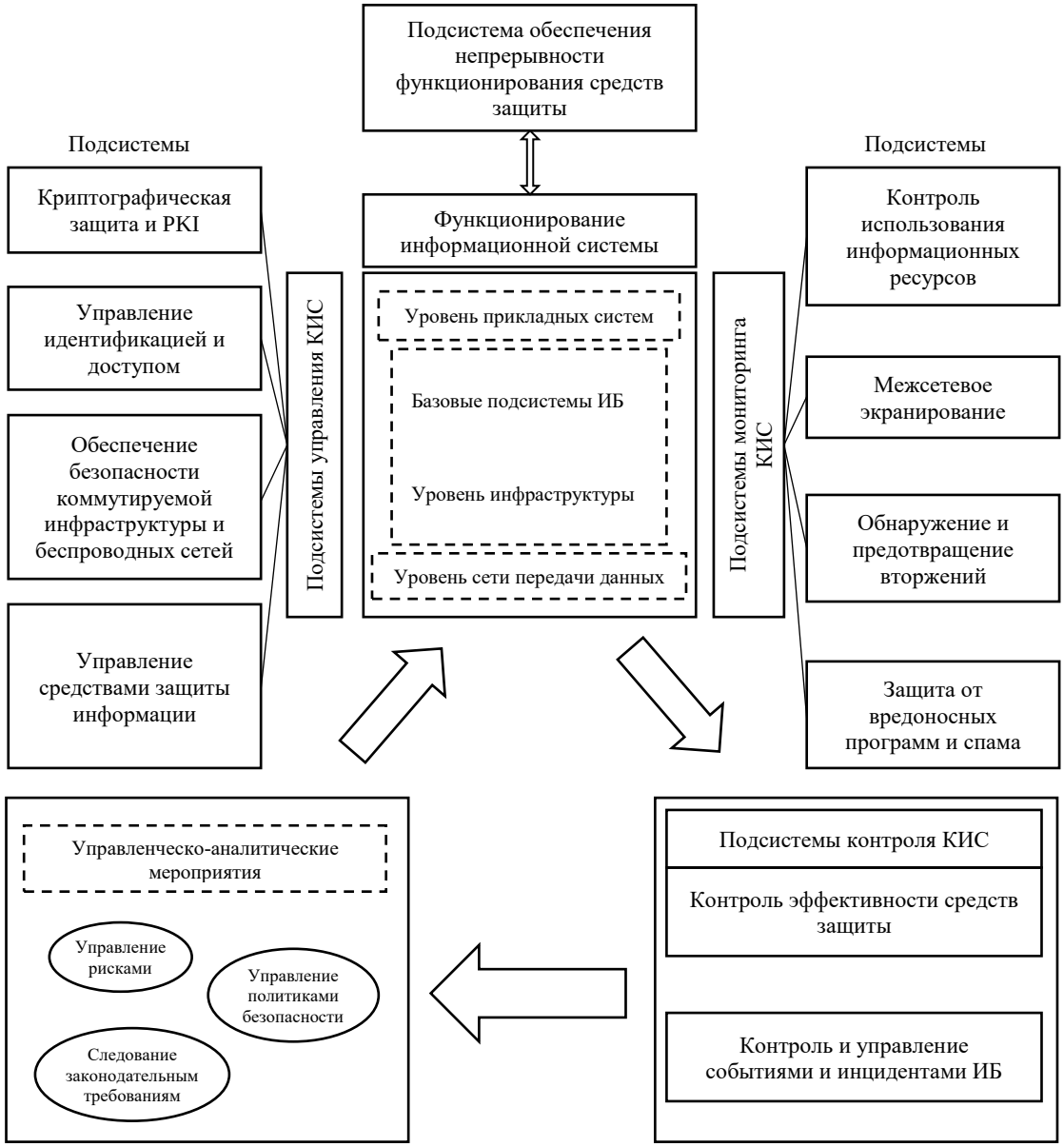


Рисунок 2 – Общая структура комплексной системы защиты информации КИС

Обеспечение безопасности информации на программно-аппаратном уровне предохраняет сведения от несанкционированного доступа и снижает риски хищения и дальнейшего неправомерного использования полученных сведений.

При выборе средств защиты данных нужно учитывать, что существует несколько принципов защиты от несанкционированного доступа. На них основана работа средств программно-аппаратной защиты:

– доступ к данным предоставляется только тем пользователям, которые уполномочены его получить на уровне внутренних документов компании;

– каждый уполномоченный пользователь имеет доступ только к своему уровню информации, его прав недостаточно для работы с данными, находящимися в сфере ответственности других пользователей;

– перечень операций, которые допустимо выполнять с данными, строго регламентирован, и зависит от изначально заданных прав пользователей [36].

Для защиты от НСД в аппаратно-программных средствах должен быть механизм распознавания уполномоченного пользователя и его авторизации (идентификации и аутентификации).

При *идентификации* пользователю необходимо передать системе свой идентифицирующий признак, например, логин и пароль [16].

При *аутентификации* программно-аппаратные средства сравнивают заявленный идентифицирующий признак пользователя с теми, которые хранятся в памяти устройства. Так устанавливается подлинность пользователя [4].

После того, как подлинность пользователя установлена, аппаратно-программным средством определяется объем предоставленных ему прав.

Исходя из этого, для защиты корпоративной информационной системы образовательной организации можно использовать следующие аппаратно-программные возможности:

1. Антивирусные программы – это программы, которые обнаруживают и удаляют вирусы и другие вредоносные программы. Они могут быть установлены на каждый компьютер в сети или на сервер [2].

2. Файрволлы – это программы или аппаратные устройства, которые контролируют трафик между компьютерами и сетями. Они могут блокировать нежелательные соединения и защищать сеть от внешних угроз [25].

3. Программы шифрования – это программы или аппаратные устройства, которые защищают данные от несанкционированного доступа путем шифрования информации.

4. Системы аутентификации – это программы или аппаратные устройства, которые проверяют личность пользователя перед предоставлением доступа к системе. Они могут использовать пароли, биометрические данные или токены.

5. Системы мониторинга – это программы или аппаратные устройства, которые мониторят производительность сети и компьютеров, а также оповещают администраторов о возможных проблемах.

Для реализации защиты корпоративной информационной системы перечисленные аппаратно-программные средства должны соответствовать необходимым требованиям и ограничениям [11]:

1. Система должна иметь достаточное количество мощных серверов и сетевых устройств для обеспечения стабильной работы и быстрого доступа к информации.

2. Необходимо учитывать законодательные требования и регуляторные нормы, связанные с защитой информации.

3. Система должна быть настроена на автоматическое обновление и проверку обновлений для всех установленных программных продуктов.

4. Система должна быть гибкой и масштабируемой, чтобы обеспечить возможность добавления новых функций и средств защиты в будущем.

5. Система должна иметь механизмы резервного копирования данных и восстановления в случае их потери или повреждения.

6. Система должна иметь механизмы мониторинга и анализа событий, чтобы быстро обнаруживать и реагировать на потенциальные угрозы.

7. Необходимо регулярно проводить аудит безопасности системы и устранять выявленные уязвимости.

8. Для защиты от несанкционированного доступа к информации необходимо использовать средства аутентификации, такие как пароли, биометрические данные и т.д.

9. Важно установить политику доступа к информации и правила использования средств защиты, чтобы минимизировать риски нарушения безопасности.

10. Необходимо учитывать особенности работы образовательной организации и ее информационных систем, чтобы выбранные средства защиты были наиболее эффективными и соответствовали требованиям.

11. Важно учитывать финансовые возможности организации при выборе средств защиты, чтобы обеспечить оптимальное соотношение цены и качества.

12. Важно проводить обучение и тренировки сотрудников по вопросам информационной безопасности, чтобы они были готовы к действиям в случае угрозы.

Дифференциация подхода к выбору средств защиты корпоративной информационной системы определяется важностью обрабатываемой информации, различием автоматизированных систем по своему составу, структуре, способам обработки информации, количественному и качественному составу пользователей и обслуживающего персонала. В соответствии с Руководящим документом ФСТЭК России «Автоматизированные системы. Защита от несанкционированного доступа к информации. Классификация автоматизированных систем и требования по защите информации» от 30 марта 1992 г. устанавливается девять классов защищенности автоматизированной системы от несанкционированного доступа к информации. Классы подразделяются на три группы, отличающиеся особенностями обработки информации в автоматизированных системах [1].

Третья группа включает автоматизированные системы (далее – АС), в которых работает один пользователь, допущенный ко всей информации АС, размещенной на носителях одного уровня конфиденциальности. Группа содержит два класса – 3Б и 3А.

Вторая группа включает АС, в которых пользователи имеют одинаковые права доступа (полномочия) ко всей информации АС, обрабатываемой и (или)

хранимой на носителях различного уровня конфиденциальности. Группа содержит два класса 2Б и 2А.

Первая группа включает многопользовательские АС, в которых одновременно обрабатывается и (или) хранится информация разных уровней конфиденциальности. Не все пользователи имеют право доступа ко всей информации АС. Группа содержит пять классов – 1Д, 1Г, 1В, 1Б и 1А.

Полная схема классификации автоматизированных систем представлена на рисунке 3.

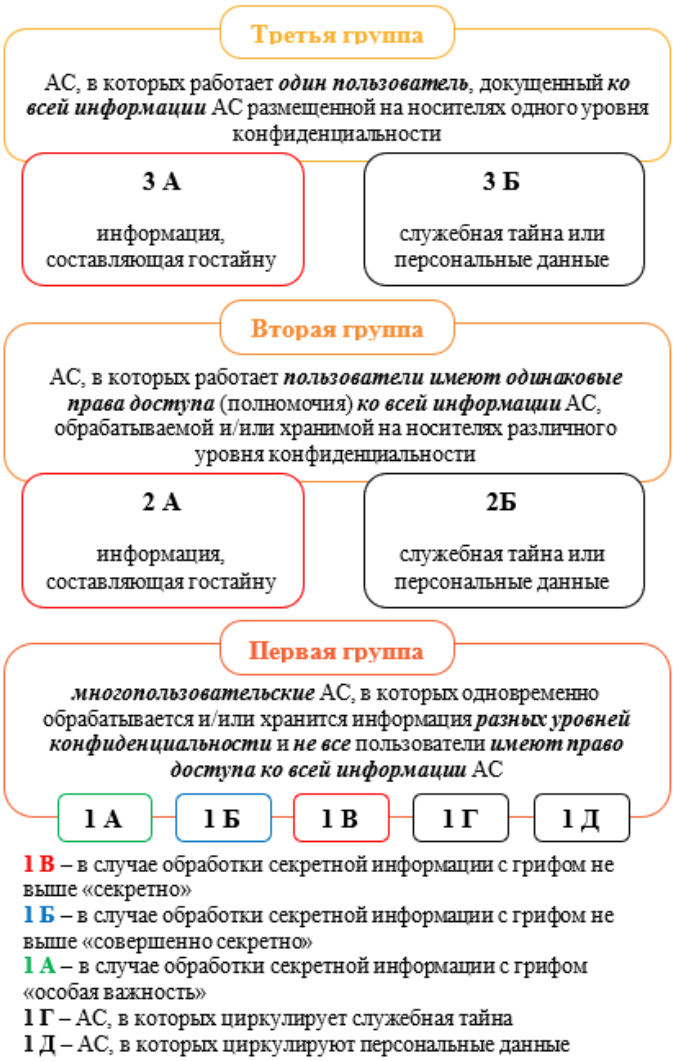


Рисунок 3 – Классификация автоматизированных систем

В образовательных организациях корпоративной информационной системой пользуются:

– администрация: директор, заместитель директора по учебно-воспитательной работе, заместитель директора по воспитательной работе,

заместитель директора по административно-хозяйственной работе, главный бухгалтер и бухгалтер;

– педагогические работники: классные руководители, преподаватели, руководители методического объединения, психолог, библиотекарь, социальный педагог;

– вспомогательный персонал: делопроизводитель, специалист по кадрам, кассир буфета и вахтёр.

В составе массивов охраняемой законом информации, находящейся в распоряжении образовательной организации, можно выделить три группы:

– персональные сведения, касающиеся обучающихся и преподавателей, оцифрованные архивы;

– ноу-хау образовательного процесса, носящие характер интеллектуальной собственности и защищенные законом;

– структурированная учебная информация, обеспечивающая образовательный процесс (библиотеки, базы данных, обучающие программы).

Следовательно, согласно схеме, в образовательных организациях резонно использовать первую группу многопользовательских АС класса 1Д.

В зависимости от класса АС в рамках этих подсистем должны быть реализованы определённые требования. В классе 1Д реализуются следующие требования:

Подсистема управления доступом:

– должна осуществляться идентификация и проверка подлинности субъектов доступа при входе в систему по паролю условно-постоянного действия длиной не менее шести буквенно-цифровых символов.

Подсистема регистрации и учета:

– должна осуществляться регистрация входа (выхода) субъектов доступа в систему (из системы), либо регистрация загрузки и инициализации операционной системы и ее программного останова.

Регистрация выхода из системы или останова не проводится в моменты аппаратурного отключения АС. В параметрах регистрации указываются:

– дата и время входа (выхода) субъекта доступа в систему (из системы) или загрузки (останова) системы;

– результат попытки входа: успешная или неуспешная - несанкционированная;

– идентификатор (код или фамилия) субъекта, предъявленный при попытке доступа;

– должен проводиться учет всех защищаемых носителей информации с помощью их маркировки и с занесением учетных данных журнала (учетную карточку);

– учет защищаемых носителей должен проводиться в журнале (картотеке) с регистрацией их выдачи (приема).

Подсистема обеспечения целостности:

– должна быть обеспечена целостность программных средств СЗИ НСД, обрабатываемой информации, а также неизменность программной среды.

При этом:

– целостность системы защиты информации (далее – СЗИ) от несанкционированного доступа (далее – НСД) проверяется при загрузке системы по контрольным суммам компонент СЗИ;

– целостность программной среды обеспечивается использованием трансляторов с языков высокого уровня и отсутствием средств модификации объектного кода программ в процессе обработки и (или) хранения защищаемой информации;

– должна осуществляться физическая охрана средств вычислительной техники (устройств и носителей информации), предусматривающая контроль доступа в помещения АС посторонних лиц, наличие надежных препятствий для несанкционированного проникновения в помещения АС и хранилище носителей информации, особенно в нерабочее время;

– должно проводиться периодическое тестирование функций СЗИ НСД при изменении программной среды и персонала АС с помощью тест - программ, имитирующих попытки НСД;

– должны быть в наличии средства восстановления СЗИ НСД, предусматривающие ведение двух копий программных средств СЗИ НСД и их периодическое обновление и контроль работоспособности.

Исходя из вышесказанного, при выборе средств защиты корпоративной информационной системы необходимо опираться на определённые принципы защиты, аппаратно-программные возможности, которые должны соответствовать необходимым требованиям и ограничениям. Опираться на степень важности обрабатываемой информации, состав корпоративной информационной системы, структуру, способы обработки информации, количественный и качественный состав пользователей и обслуживающего персонала.

Таким образом, осуществление защиты должно быть комплексным, включающим в себя защиту централизованного управления, приложений и соответствующих серверов, сети и конечных пользователей. Комплексная защита представляет собой целостный и достаточный набор средств защиты от актуальных угроз информационной безопасности, который интегрируется в защищаемую информационную систему.

Вывод по первой главе

В первой главе были рассмотрены научно-методические основы корпоративной информационной системы и значение её защиты в образовательной организации. Были изучены нормативно-правовые требования к выбору средств защиты корпоративной информационной системы образовательной организации. Были выявлены виды средств защиты корпоративной информационной системы образовательной организации.

Понятийно информационная система представляет собой взаимосвязанную совокупность средств, методов и персонала, используемых для хранения, обработки и выдачи информации в интересах достижения поставленной цели, что подтверждает в своих исследованиях А. А. Забуга, который характеризует информационную систему, как систему способную упорядочить и скоординировать информацию так, как это необходимо для управляющего субъекта.

Проанализировав толкования Н. Н. Федякова, С. А. Шехматов, Т. Ш. Шихнабиева, И. Ю. Юханова, А. М. Ямалетдинова , А. И. Яценко было выявлено, что корпоративная информационная система – это открытая интегрированная система реального времени, автоматизирующая бизнес-процессы предприятия всех уровней и направлений деятельности, в том числе бизнес-процессы принятия управленческих решений.

Корпоративная информационная система в образовательной организации обеспечивает взаимодействие всех ее структурных подразделений, создавая единое образовательное пространство.

Таким образом корпоративная информационная система образовательной организации выступает одним из наиболее значимых классов информационных систем, подлежащих защите.

Информационная безопасность – это комплекс мер различного характера, направленных на реализацию защиты персональных данных и информационного пространства от несанкционированных вмешательств,

хищения информации и изменения конфигурации системы со стороны третьих лиц и на защиту обучающихся от любых видов пропаганды и рекламы, запрещенной законом информации.

Для защиты корпоративной информационной системы необходимо определить перечень угроз для каждого существующего в организации информационного потока; определить для каждого существующего информационного потока функционирующих в организации механизмов защиты и их достаточности; выбрать для существующего информационного потока надёжные средства защиты информации, позволяющие нейтрализовать «незакрытые» угрозы.

Информационная безопасность образовательных организаций отличается от других предприятий и организаций. В соответствии с этим, вопрос организации защиты корпоративной информационной системы образовательной организации диктует свои нормативно-правовые требования.

Законодательство в области обеспечения информационной безопасности представлено различными нормативно-правовыми актами, включая Федеральные Законы, Постановления Правительства, Указы Президента, ведомственные приказы и руководящие документы Федеральной службы по техническому и экспортному контролю (ФСТЭК России), Федеральной службы безопасности Российской Федерации (ФСБ России).

Анализируя виды средств защиты корпоративной информационной системы было выявлено, что противодействие многочисленным угрозам должно быть комплексным. Также дифференциация подхода к выбору средств защиты должна определяться важностью обрабатываемой информации, различием автоматизированных систем по своему составу, структуре, способам обработки информации, количественному и качественному составу пользователей и обслуживающего персонала.

ГЛАВА 2. РАЗРАБОТКА РЕКОМЕНДАЦИЙ ПО ВЫБОРУ СРЕДСТВ ЗАЩИТЫ КОРПОРАТИВНОЙ ИНФОРМАЦИОННОЙ СИСТЕМЫ ОБРАЗОВАТЕЛЬНОЙ ОРГАНИЗАЦИИ

2.1 Анализ защиты корпоративной информационной системы образовательной организации ГБПОУ «Южно-Уральский государственный технический колледж»

В качестве объекта защиты было выбрано Государственное бюджетное профессиональное образовательное учреждение «Южно-Уральский государственный технический колледж». Местонахождение главного учебного корпуса: 454007, г. Челябинск, ул. Горького, 15. Учебного комплекса №2: 454007, г. Челябинск, ул. Грибоедова, д. 45. Машиностроительного комплекса: г. Челябинск, ул. Марченко, д. 33. Политехнического комплекса: г. Челябинск, ул. Гагарина, д. 7.

В колледже реализуются образовательные программы среднего профессионального образования, основные программы профессионального обучения, дополнительные общеобразовательные и профессиональные программы, услуги по содержанию и воспитанию обучающихся в общежитии, организация и проведение мероприятий в сфере образования и науки.

Основные задачи колледжа определяются в соответствии с нормативно-правовыми актами Российской Федерации и реализуются в соответствии с Уставом колледжа [37]:

– удовлетворение потребностей граждан в получении профессионального образования в избранной профессиональной деятельности, в интеллектуальном, культурном, физическом и нравственном развитии;

– удовлетворение потребностей общества в профессионально подготовленных специалистах, создании новых рабочих мест;

– профессиональная переподготовка и повышение квалификации специалистов и рабочих;

– распространение знаний среди населения, повышение его общеобразовательного и культурного уровня, в том числе путем оказания платных образовательных услуг.

В своей образовательной деятельности колледж использует наиболее эффективные технологии обучения и воспитательные системы.

Доступ педагогических работников к информационно-телекоммуникационной сети Интернет в колледже осуществляется с персональных компьютеров (ноутбуков и т.п.), подключенных к сети Интернет, без ограничения времени и потребленного трафика.

Для доступа к информационно-телекоммуникационным сетям в колледже педагогическому работнику предоставляются идентификационные данные (логин и пароль). Предоставление доступа осуществляется системным администратором колледжа.

Доступ к электронным базам данных осуществляется на условиях, указанных в договорах, заключенных колледжем с правообладателем электронных ресурсов (внешние базы данных).

Информация об образовательных, методических, научных, нормативных и других электронных ресурсах, доступных к пользованию, размещена на сайте колледжа.

В ходе учебного процесса применяются дистанционные образовательные технологии с использованием таких систем как e.lanbook.ru, moodle, dom.sustec.ru.

Для осуществления дистанционной образовательной деятельности, размещения информации о предстоящих и прошедших мероприятиях и информирования студентов об актуальных событиях у ГБПОУ «Южно-Уральский государственный технический колледж» имеется собственный сайт (режим доступа: https://sustec.ru), отвечающий всем требованиям к подобным ресурсам образовательных организаций.

Педагогическим работникам обеспечивается доступ к следующим электронным базам данных: корпоративная информационная система; информационные справочные системы; поисковые системы.

Корпоративная информационная система состоит из пяти уровней:

1. Информационно-логический уровень представляет собой совокупность потоков данных и узлов возникновения, потребления и модификации информации. Уровень представляется в виде информационно-логической модели, на основании которой разрабатываются структуры баз данных, системные соглашения и организационные правила для обеспечения взаимодействия компонентов прикладного программного обеспечения.

2. Прикладной уровень представляет собой совокупность прикладных программ и программных комплексов, которые обеспечивают реализацию функций корпоративного управления. Наиболее развитые корпоративные информационные системы используют следующие прикладные программные средства:

– программные комплексы корпоративных информационных систем (1С: Предприятие 8.0, Галактика, Парус, Босс-Корпорация и др.);

– системы управления базами данных (СУБД) и программные средства для работы с хранилищами данных (MS SQL Server, Oracle, Pervasive SQL);

– программные средства для организации корпоративного управления, интерактивного общения, совместного использования справочников и документальных баз данных;

– программные средства управления документооборотом;

– программные средства календарного планирования;

– программные комплексы для ведения конструкторских работ (САПР);

– программные средства электронного офиса (MS Qffice);

– специальные системы бизнес-планирования и анализа (Project Expert, Audit Expert, Marketing Expert);

– информационно-аналитические системы (Deductor).

3. Системный уровень описывает операционные системы и сетевое программное обеспечение, которые составляют рекомендуемое программное окружение для программного комплекса корпоративных информационных систем.

4. Аппаратный уровень описывает средства вычислительной техники, требования к конфигурации серверов, рабочих станций.

5. Транспортный уровень определяет активное и пассивное сетевое оборудование, сетевые протоколы и технологии [4].

К Южно-Уральскому государственному техническому колледжу относятся различные информационные системы, которые используются для управления образовательным процессом и обеспечения коммуникации между преподавателями и студентами:

1. Система электронного документооборота – используется для обмена документами между участниками образовательного процесса.

2. Система электронного расписания – позволяет студентам и преподавателям получать доступ к расписанию занятий и изменениям в нем.

3. Система электронной почты – обеспечивает коммуникацию между преподавателями и студентами.

4. Система дистанционного обучения – позволяет студентам получать доступ к учебным материалам и заданиям в любое время и из любого места.

5. Система управления базами данных – используется для хранения и управления информацией о студентах, преподавателях и учебных материалах.

6. Система электронной библиотеки – позволяет студентам получать доступ к электронным версиям учебников и научных статей.

Согласно исследованию, защита данных информационных систем является необходимым условием при организации управления образовательным процессом и коммуникации.

Целостность информационных систем образовательных организаций подвержена различным угрозам.

Источники угроз – это потенциальные антропогенные, техногенные и стихийные угрозы безопасности. В качестве источников угроз могут выступать как субъекты (личность), так и объективные проявления [17].

Под угрозой в целом понимают потенциально возможное событие, действие (воздействие), процесс или явление, которое может привести к нанесению ущерба чьим – либо интересам.

Все источники угроз информационной безопасности можно разделить на три основные группы (рисунок 4) [21].

I. Обусловленные действиями субъекта (антропогенные источники), которые могут привести к нарушению безопасности информации. Данные действия могут быть квалифицированы как умышленные (преднамеренные) или случайные (непреднамеренные) преступления. Источники, действия которых могут привести к нарушению безопасности информации, бывают как внешними, так и внутренними. Данные источники можно спрогнозировать и принять адекватные меры.

II. Обусловленные техническими средствами (техногенные источники). Эти источники угроз менее прогнозируемы и напрямую зависят от свойств техники и поэтому требуют особого внимания. Данные источники угроз информационной безопасности также могут быть как внутренними, так и внешними.

III. Стихийные источники. Данная группа объединяет обстоятельства, составляющие непреодолимую силу (стихийные бедствия или другие обстоятельства, которые невозможно предусмотреть или предотвратить, или возможно предусмотреть, но невозможно предотвратить). Эти обстоятельства носят объективный и абсолютный характер, распространяющийся на всех. Такие источники угроз совершенно не поддаются прогнозированию, и поэтому меры против них должны применяться всегда. Стихийные источники

как правило, являются внешними по отношению к защищаемому объекту и под ними, как правило, понимаются природные катаклизмы.

Рисунок 4 – Классификация источников угроз

Угрозы как возможные опасности совершения какого-либо действия, направленного против объекта защиты, проявляются не сами по себе, а через уязвимости.

Уязвимости присущи объекту информатизации, неотделимы от него и обуславливаются недостатками процесса функционирования, свойствами архитектуры автоматизированных систем, протоколами обмена и интерфейсами, применяемыми программным обеспечением и аппаратной платформой, условиями эксплуатации и расположения и т.п.

Уязвимости могут присутствовать как в программно-аппаратном, так и организационно-правовом обеспечении корпоративной информационной системы.

Основная часть уязвимостей организационно-правового обеспечения обусловлена отсутствием в организации нормативных документов, касающихся вопросов информационной безопасности. Примером уязвимости данного типа является отсутствие в организации утверждённой концепции или политики информационной безопасности, которая бы определяла требования к защите информационной системы, а также конкретные пути их реализации.

Уязвимости программно-аппаратного обеспечения могут присутствовать в программных или аппаратных компонентах рабочих станций пользователей информационной системы, серверов, а также коммуникационного оборудования и каналов связи информационной системы.

Источники угроз могут использовать уязвимости для нарушения безопасности информации, получения незаконной выгоды (нанесения ущерба собственнику, владельцу, пользователю информации). Кроме того, возможны незлонамеренные действия источников угроз по активизации тех или иных уязвимостей, способных нанести вред.

Каждой угрозе могут быть сопоставлены различные уязвимости. Устранение или существенное ослабление уязвимостей влияет на возможность реализации угроз безопасности информации.

Существуют следующие уязвимости информационных систем:

– объективные;
– субъективные;
– случайные.

Объективные уязвимости зависят от особенностей построения и технических характеристик оборудования, применяемого на защищаемом объекте. Полное устранение этих уязвимостей невозможно, но они могут существенно ослабляться техническими и инженерно-техническими методами парирования угроз безопасности информации.

Субъективные уязвимости зависят от действий сотрудников и, в основном, устраняются организационными и программно-аппаратными методами.

Случайные уязвимости зависят от особенностей окружающей защищаемый объект среды и непредвиденных обстоятельств. Эти факторы, как правило, мало предсказуемы и их устранение возможно только при проведении комплекса организационных и инженерно-технических мероприятий по противодействию угрозам информационной безопасности.

Из-за уязвимостей на корпоративную информационную систему образовательной организации могут быть совершены следующие типы атак:

– пассивная;
– активная.

К пассивной атаке относят атаку, при которой противник не имеет возможности модифицировать передаваемые сообщения и вставлять в информационный канал между отправителем и получателем свои сообщения. Целью пассивной атаки может быть только прослушивание передаваемых сообщений и анализ трафика.

А активным атакам относят атаку, при которой противник имеет возможность модифицировать передаваемые сообщения и вставлять свои сообщения. К типам активных атак относят:

– Backdoor;
– Фишинг;
– Переадресация маршрутов;
– Взлом удалённого доступа;
– DoS-атака;

Backdoor – вредоносная программа, а иногда намеренно оставленная лазейка в коде легальной программы, которая предоставляет доступ к устройству для несанкционированных действий. Бэкдор в точности соответствует своему названию (от англ. back door – «черный ход»): скрытно впускает злоумышленника в систему, наделяя правами администратора.

Успешные атаки дают киберпреступнику доступ к устройству и позволяют перехватывать и подменять трафик.

Кроме непосредственного управления процессами на уровне системы и даже Bios, бэкдоры могут воровать персональные данные пользователя, скачивать и отправлять по сети файлы, открывать доступ для вирусов и червей, подключаться к удаленным хостам, превращать компьютер в «зомби», делая его частью ботнета, и все это незаметно [53].

Межсетевые экраны способны отфильтровывать исходящий трафик, что лишает программ-шпионов и «троянских коней» возможности связываться с пославшими их злоумышленниками, однако для этого необходимо задать несколько неочевидных правил фильтрации.

Фишинг относится к числу наиболее распространённых видов интернет-мошенничества. Он связан с похищением конфиденциальной информации у пользователя путем обмана или манипуляции. В качестве цели злоумышленники ставят получение и сбор личных сведений, которые могут быть проданы третьей стороне или использованы для личного обогащения. Осуществляется путем установки вредоносного программного обеспечения, предоставляющего удалённый доступ к устройству пользователя, или прямого хищения данных через незащищённый канал связи.

Существуют следующие виды фишинга, которые характерны для корпоративной информационной системы:

1. *Почтовый*. Заключается в массовой рассылке писем на электронные ящики с различными привлекательными сообщениями. Например, выигрыш в лотерее, получение подарка, предоставление бесплатных и прочих услуг. Для этого требуется перейти по ссылке и ввести свои данные, после чего они похищаются.

2. *Целевой*. Конкретным людям, представляющим ценность для мошенника, отправляются персонализированные письма. Мошенник входит в глубокое доверие, формирует дружеские и партнерские отношения вследствие чего жертва добровольно расстается со сведениями.

3. *Фарминг*. Атаке хакеров подвергаются DNS-серверы: пользователь получает ссылку не настоящий интернет-ресурс, а на мошеннический сайт, где вводит личную информацию, открывая тем самым доступ к конфиденциальным данным.

4. *Клон-фишинг*. Заключается в отправке на электронную почту жертвы скопированного и воспроизведенного письма, которое было получено до этого от легитимного отправителя. Во втором письме происходит подмена контактов и ссылок, что чревато при переходе по ним потерей конфиденциальной личной информации [44].

Эффективным решением для организации безопасности от фишинга является внедрение системы защиты конечных точек, но данные системы имеют высокую стоимость и относительно сложную процедуру установки и высококвалифицированного персонала, поэтому не все организации могут использовать их. Выходом из ситуации является использование комплексных средств защиты, так как они способны оказывать противодействие данным атакам.

В переадресации маршрута пакеты данных передаются по сети определенными маршрутами, а этот вид атак предполагает подмену пути следования информации таким образом, чтобы конечное устройство ничего не «заподозрило». Межсетевой экран отследит атаку и перекроет канал трафика [25].

Взлом удаленного доступа подразумевает перехват злоумышленниками трафика управления удаленным доступом и взломом устройства, передающего этот трафик. Этого можно добиться с помощью троянов удаленного доступа, которые позволяют злоумышленнику получить контроль над компьютером жертвы. Получив доступ к зараженному компьютеру, автор трояна может изучать вашу файловую систему, просматривать ваши действия на экране, собирать ваши учетные данные для входа на различные ресурсы, просматривать входящий поток из веб-камеры, а также просто запустить процесс шифрования файлов с требованием выкупа. В отличии от

официальных программ для удаленного доступа, трояны маскируются под обычные исполняемые файлы, которые обычно пользователь скачивает из сети Интернет. Получается, что в «полезную нагрузку» вместе с нужно программой идет еще и троян.

Антивирусное программное обеспечение может оказаться бесполезно против трояна удаленного доступа, ведь сами трояны выдают себя как нечто законное. Поэтому лучше всего обнаружить трояны удаленного доступа могут грамотно настроенные межсетевые экраны [42].

Атака типа «отказ в обслуживании» (DoS) – это попытка причинить вред, сделав недоступной целевую систему, например веб-сайт или приложение, для обычных конечных пользователей. Обычно злоумышленники генерируют большое количество пакетов или запросов, которые в конечном счете перегружают работу целевой системы [46].

Первым делом злоумышленник сканирует крупную сеть с помощью специально подготовленных сценариев, которые выявляют потенциально слабые узлы. Выбранные узлы подвергаются нападению, и злоумышленник получает на них права администратора. На захваченные узлы устанавливаются троянские программы, которые работают в фоновом режиме [18]. Теперь эти компьютеры называются компьютерами-зомби, их пользователи даже не подозревают, что являются потенциальными участниками DDoS-атаки. Далее злоумышленник отправляет определенные команды захваченным компьютерам и те, в свою очередь осуществляют коллективную DoS-атаку на целевой компьютер.

Защититься от Dos-атак можно с помощью фильтрации, т.е. блокирования трафика, исходящего от атакующих машин. Эффективность этих методов снижается по мере приближения к объекту атаки и повышается по мере приближения к атакующей машине. Использование межсетевых экранов блокирует конкретный поток трафика, но не позволяет отделить «хороший» трафик от «плохого». Поскольку главная задача брандмауэра – это фильтрация, он помогает справиться с наплывом огромных объемов трафика.

Блокировка работает как на входящие, так и на исходящие пакеты, если ваше устройство попробуют использовать в качестве атакующего [25].

Межсетевые экраны реализуют методы контроля за информацией, поступающей и/или выходящей из информационной системы, и обеспечивают защиту посредством фильтрации информации на основе критериев, заданных администратором.

Процедура фильтрации включает в себя анализ заголовков каждого пакета, проходящего через межсетевой экран, и передачу его дальше по маршруту следования только в случае, если он удовлетворяет заданным правилам фильтрации. При помощи фильтрования межсетевые экраны позволяют обеспечить защиту от сетевых атак путём удаления из информационного потока тех пакетов данных, которые представляют потенциальную опасность для информационной системы.

Для проведения анализа уязвимостей корпоративной информационной системы ГБПОУ «Южно-Уральского государственного технического колледжа» наиболее оптимальным методом является разработка модели угроз.

Необходимость разработки модели угроз регламентирована рядом нормативных документов, таких как:

1. Часть 2 статьи 19 закона No152-ФЗ «О персональных данных», где говорится, что обеспечение безопасности персональных данных достигается, в частности: определением угроз безопасности персональных данных при их обработке в информационных системах персональных данных» [27].

2. Состав и содержание организационных и технических мер по обеспечению безопасности персональных данных при их обработке в информационных системах персональных данных (утверждены приказом Федеральной службы по техническому и экспортному контролю России (ФСТЭК России) от 18 февраля 2013г. No 21): «Меры по обеспечению безопасности персональных данных реализуются, в том числе посредством применения в информационной системе средств защиты информации, прошедших в установленном порядке процедуру оценки соответствия, в

случаях, когда применение таких средств необходимо для нейтрализации актуальных угроз безопасности персональных данных» [30].

3. Требования о защите информации, не составляющей государственную тайну, содержащейся в государственных информационных системах (утверждены ФСТЭК России от 11 февраля 2013г. No 17): «Формирование требований к защите информации включает: определение угроз безопасности информации, реализация которых может привести к нарушению безопасности информации в информационной системе, и разработку на их основе модели угроз безопасности информации» [30].

Отсюда следует вывод: для любых корпоративных информационных систем, так или иначе подлежащих защите в соответствии с законодательством необходимо разработать модель угроз.

Таким образом, модель угроз информационной безопасности автоматизированной системы должна содержать:

- описание информационной системы;
- структурно-функциональные характеристики;
- описание угроз безопасности;
- модель нарушителя;
- возможные уязвимости;
- способы реализации угроз;
- последствия от нарушения свойств безопасности информации.

Для модели угроз изначально определяется глобальный параметр – уровень исходной защищенности. Определяется он один раз и не меняется от угрозы к угрозе. Чтобы определить уровень исходной защищенности (он же коэффициент исходной защищенности Y1) нужно для семи показателей выбрать одно из значений, которое больше всего подходит для вашей системы.

Каждому значению соответствует высокий, средний или низкий уровень защищенности. Считаем какой процент у нас получился для показателей с разными значениями. Если «высокий» и «средний» набрали 70% и выше, то

определяем средний уровень исходной защищенности (Y1 = 5), если нет, то – низкий (Y1 = 10).

Далее необходимо определить частоту (вероятность) реализации угрозы (коэффициент Y2) – показатель, характеризующий, насколько вероятным является реализация конкретной угрозы безопасности ПДн для данной ИСПДн в складывающихся условиях обстановки. Вводятся четыре вербальных градации этого показателя:

– маловероятно – отсутствуют объективные предпосылки для осуществления угрозы (например, угроза хищения носителей информации лицами, не имеющими легального доступа в помещение, где последние хранятся);

– низкая вероятность – объективные предпосылки для реализации угрозы существуют, но принятые меры существенно затрудняют ее реализацию (например, использованы соответствующие средства защиты информации);

– средняя вероятность – объективные предпосылки для реализации угрозы существуют, но принятые меры обеспечения безопасности ПДн недостаточны;

– высокая вероятность – объективные предпосылки для реализации угрозы существуют и меры по обеспечению безопасности ПДн не приняты.

При составлении перечня актуальных угроз безопасности ПДн каждой градации вероятности возникновения угрозы ставится в соответствие числовой коэффициент, а именно:

– 0 – для маловероятной угрозы;

– 2 – для низкой вероятности угрозы;

– 5 – для средней вероятности угрозы;

– 10 – для высокой вероятности угрозы.

Следующий столбец – коэффициент реализуемости угрозы Y. Вычисляется по простой формуле:

$$Y = (Y1+Y2)/20.$$

Возможность реализации – это вербальный аналог коэффициента Y. Определяется в зависимости от числового значения следующим образом:

– если $0 \leq Y \leq 0{,}3$, то возможность реализации угрозы признаётся низкой;

– если $0{,}3 \leq Y \leq 0{,}6$, то возможность реализации угрозы признаётся средней;

– если $0{,}6 < Y \leq 0{,}8$, то возможность реализации угрозы признаётся высокой;

– если $Y > 0{,}8$, то возможность реализации угрозы признаётся очень высокой.

Следующий столбец – актуальность угрозы. Определяется по таблице правил отнесения угрозы безопасности ПДн к актуальной (таблица 1).

Таблица 1 – Правила отнесения угрозы безопасности ПДн к актуальной

Возможность реализации угрозы	Показатель опасности угрозы		
	Низкая	Средняя	Высокая
Низкая	неактуальная	неактуальная	актуальная
Средняя	неактуальная	актуальная	актуальная
Высокая	актуальная	актуальная	актуальная
Очень высокая	актуальная	актуальная	актуальная

В результате была разработана модель угроз для ГБПОУ «Южно-Уральского государственного технического колледжа», представленная в приложении А. В модели угроз отражены все возможные угрозы корпоративной информационной системе образовательной организации, дана вероятностная оценка реализации угрозы и представлены возможные меры по исключению риска наступления данного события.

2.2 Разработка рекомендаций по выбору средств защиты корпоративной информационной системы образовательной организации ГБПОУ «Южно-Уральский государственный технический колледж»

В пункте 1.3 главы 1 было выявлено, что осуществление защиты должно быть комплексным с целостным и достаточным набором средств защиты от актуальных угроз.

Согласно словам ведущего эксперта компьютерно-технического направления в компании RTM Group Федора Музалевского «Ни одно программное решение не защищает информацию полностью – оно блокирует одни возможности атаки, но оставляет пространство для других. Для построения эффективной системы защиты информации нужно подбирать несколько программных средств и выстраивать комплекс, где каждое средство «прикрывает тылы» другого. Только в этом случае ваша информация будет полностью защищена» [35].

Сегодня на рынке основным и наиболее востребованным организациями элементом сетевой безопасности являются многофункциональные межсетевые экраны нового поколения NGFW (Next Generation Firewall) или многофункциональные шлюзы безопасности UTM (Unified Threat Management), которые обеспечивают комплексную защиту от сетевых угроз. В последние годы обозначение UTM постепенно заменяется на более понятный и соответствующий реальным задачам термин – многофункциональные шлюзы безопасности USG (Unified Security Gateway).

С появлением межсетевых экранов нового поколения, в которых правила межсетевого экрана стало возможным создавать на уровне приложения (L7 в сетевой модели OSI), все изменилось. Появилась вторая ветвь развития функциональности – в сторону работы на прикладном уровне.

Современные продукты класса USG покрывают функциональность большого количества отдельных классов решений для сетевой безопасности, представляя собой необходимый набор инструментов с гибкими настройками в рамках одного физического устройства или аппаратной платформы.

Универсальные шлюзы безопасности с единой консолью управления позволяют организациям повысить уровень контроля, исключают рутинные операции, связанные с эксплуатацией большого количества отдельных узкоспециализированных систем, и позволяют организациям двигаться в сторону перехода от отдельных решений к комплексной и интегрированной защите от сложных угроз.

Межсетевой экран, сетевой экран – программный или программно-аппаратный элемент компьютерной сети, осуществляющий контроль и фильтрацию проходящего через него сетевого трафика в соответствии с заданными правилами [25].

Среди задач, которые решают межсетевые экраны, основной является защита сегментов сети или отдельных хостов от несанкционированного доступа с использованием уязвимых мест в протоколах сетевой модели OSI или в программном обеспечении, установленном на компьютерах сети. Межсетевые экраны пропускают или запрещают трафик, сравнивая его характеристики с заданными шаблонами.

Функции межсетевого экрана включают в себя:

– Защиту корпоративной сети от внешних угроз, например – атак, в ходе которых злоумышленники генерируют большое количество запросов с целью перегрузить сеть. Межсетевой экран определяет узлы, с которых проводится атака, и блокирует их.

– Блокировку передачи информации неизвестным источникам. Межсетевой экран не позволяет информации покинуть систему, если адресат неизвестен, находится в черном списке или проявляет повышенную активность в отношении важных данных.

– Обнаружение и блокировку подменного трафика. Межсетевой экран анализирует и проверяет трафик, выявляя попытки проникновения в корпоративную сеть со стороны подозрительных и неизвестных адресатов, которые пытаются перехватить данные. Блокировка осуществляется по IP-адресу или портам [22].

Межсетевой экран защищает от Backdoor-атак, фишинга, переадресации маршрутов, взлома удалённого доступа, DDoS-атак.

Наиболее распространённое место для установки межсетевых экранов – граница периметра локальной сети для защиты внутренних хостов от атак извне. Однако атаки могут начинаться и с внутренних узлов – в этом случае, если атакуемый хост расположен в той же сети, трафик не пересечёт границу

сетевого периметра, и межсетевой экран не будет задействован. Поэтому в настоящее время межсетевые экраны размещают не только на границе, но и между различными сегментами сети, что обеспечивает дополнительный уровень безопасности.

Разрешение или запрет доступа межсетевым экраном осуществляется на основе заданных администратором параметров. В том числе могут использоваться следующие параметры и их комбинации:

– IP-адреса. При помощи Firewall можно предоставить или запретить получение пакетов с определенного адреса или задать перечень запрещенных и разрешенных IP-адресов.

– Доменные имена. Возможность установки запрета на пропуск трафика с определенных веб-сайтов.

– Порты. Задание перечня запрещенных и разрешенных портов позволяет регулировать доступ к определенным сервисам и приложениям. Например, заблокировав порт 80, можно запретить доступ пользователей к веб-сайтам.

– Протоколы. Межсетевой экран может быть настроен таким образом, чтобы блокировать доступ трафика определенных протоколов.

Для защиты локальных сетей от нежелательного трафика и несанкционированного доступа применяются различные виды межсетевых экранов. В зависимости от способа реализации, они могут быть программными или программно-аппаратными.

Программный Firewall – это специальный софт, который устанавливается на компьютер и обеспечивает защиту сети от внешних угроз. Это удобное и недорогое решение для частных ПК, а также для небольших локальных сетей – домашних или малого офиса. Они могут применяться на корпоративных компьютерах, используемых за пределами офиса.

Для защиты более крупных сетей используются программные комплексы, под которые приходится выделять специальный компьютер. При этом требования по техническим характеристикам к таким ПК являются

довольно высокими. Использование мощных компьютеров только под решение задач МСЭ нельзя назвать рациональным. Да и производительность файервола часто оставляет желать лучшего [24].

Поэтому в крупных компаниях и организациях обычно применяют аппаратно-программные комплексы. Это специальные устройства, которые, как правило, работают на основе операционных систем FreeBSD или Linux.

Функционал таких устройств строго ограничивается задачами межсетевого экрана, что делает их применение экономически оправданным.

Применение программно-аппаратных комплексов характеризуется следующими преимуществами:

– повышенная производительность за счет того, что операционная система работает целенаправленно на выполнение одной функции;

– простота в управлении. Контролировать работу можно через любой протокол, в том числе стандартный (SNMP, Telnet) или защищенный (SSH, SSL);

– повышенная надежность защиты за счет высокой отказоустойчивости программно-аппаратных комплексов.

Образовательная организация хранит персональные данные. Согласно 152-ФЗ, она обязана обеспечить им защиту. Чтобы защищать данные в соответствии с требованиями закона, организации нужно использовать средства защиты, сертифицированные ФСТЭК. Такой сертификат подтверждает, что программа или устройство действительно надежно защищает данные. ФСТЭК сертифицирует в том числе межсетевые экраны – как программные, так и аппаратные [6].

Для сертификации межсетевого экрана ФСТЭК определяет его профиль защиты. Профиль нужно знать, чтобы понять, в какой конкретно системе, с какими целями и для защиты каких данных можно использовать этот экран.

К каждому профилю есть конкретные технические требования, а сам профиль зависит от двух параметров: типа МЭ и его класса защиты [38].

Типы межсетевых экранов по ФСТЭК:

– «А» – аппаратные, установленные на физических границах сети. Например, программно-аппаратные комплексы в месте физического подключения сети компании к интернету через кабель;

– «Б» – программные и аппаратные, установленные на логических границах сети, например встроенные в маршрутизатор;

– «В» – программные, установленные на узлы, например компьютеры сотрудников;

– «Г» – аппаратные и программные, работающие с протоколами http и https, то есть с веб-трафиком;

– «Д» – аппаратные и программные, которые работают с промышленными протоколами передачи данных.

Классы защиты межсетевых экранов по ФСТЭК:

– 6 класс – самый низший, подходит для работы с персональными данными 3 и 4 уровня защищенности.

– 5 класс – подходит для работы с данными 2 уровня защищенности.

– 4 класс – подходит для работы с данными 1 уровня защищенности.

– 1, 2 и 3 класс – необходим для работы с гостайной.

Чаще всего межсетевой экран устанавливают на границе корпоративной сети и интернета, следовательно, для образовательной организации подойдёт межсетевой экран типа «А».

Согласно Постановлению Правительства РФ от 01.11.2012 N 1119 «Об утверждении требований к защите персональных данных при их обработке в информационных системах персональных данных», угрозы 3-го типа актуальны для информационной системы, если для нее актуальны угрозы, не связанные с наличием недокументированных (недекларированных) возможностей в системном и прикладном программном обеспечении, используемом в информационной системе [32].

Необходимость обеспечения 4-го уровня защищенности персональных данных при их обработке в информационной системе устанавливается при наличии хотя бы одного из следующих условий:

а) для информационной системы актуальны угрозы 3-го типа и информационная система обрабатывает общедоступные персональные данные;

б) для информационной системы актуальны угрозы 3-го типа и информационная система обрабатывает иные категории персональных данных сотрудников оператора или иные категории персональных данных менее чем 100000 субъектов персональных данных, не являющихся сотрудниками оператора.

Следовательно, для работы с персональными данными 4 уровня защищенности подходит 6 класс межсетевых экранов.

Согласно таблице определения профиля межсетевого экрана (рисунок 5) для межсетевого экрана типа «А» 6 класса защиты подходит идентификатор профиля защиты ИТ.МЭ.А6.ПЗ 9.

Класс защиты Тип межсетевого экрана	6	5	4	3	2	1
Межсетевой экран типа "А"	ИТ.МЭ. А6.ПЗ	ИТ.МЭ. А5.ПЗ	ИТ.МЭ. А4.ПЗ	ИТ.МЭ. А3.ПЗ	ИТ.МЭ. А2.ПЗ	ИТ.МЭ. А1.ПЗ
Межсетевой экран типа "Б"	ИТ.МЭ. Б6.ПЗ	ИТ.МЭ. Б5.ПЗ	ИТ.МЭ. Б4.ПЗ	ИТ.МЭ. Б3.ПЗ	ИТ.МЭ. Б2.ПЗ	ИТ.МЭ. Б1.ПЗ
Межсетевой экран типа "В"	ИТ.МЭ. В6.ПЗ	ИТ.МЭ. В5.ПЗ	ИТ.МЭ. В4.ПЗ	ИТ.МЭ. В3.ПЗ	ИТ.МЭ. В2.ПЗ	ИТ.МЭ. В1.ПЗ
Межсетевой экран типа "Г"	ИТ.МЭ. Г6.ПЗ	ИТ.МЭ. Г5.ПЗ	ИТ.МЭ. Г4.ПЗ	-	-	-
Межсетевой экран типа "Д"	ИТ.МЭ. Д6.ПЗ	ИТ.МЭ. Д5.ПЗ	ИТ.МЭ. Д4.ПЗ	-	-	-

Рисунок 5 – Таблица определения профиля межсетевого экрана

В соответствии с методическим документом «Профиль защиты межсетевых экранов типа «А» шестого класса защиты. ИТ.МЭ.А6.ПЗ» утвержденного ФСТЭК России 12 сентября 2016 г. в межсетевых экранах должны быть реализованы следующие функции безопасности [39]:

– контроль и фильтрация;

– идентификация и аутентификация;

– регистрация событий безопасности (аудит);

– обеспечение бесперебойного функционирования и восстановление;

– управление (администрирование).

Состав функциональных требований безопасности обеспечивает следующие функциональные возможности межсетевого экрана типа «А»:

– возможность осуществлять фильтрацию сетевого трафика для отправителей информации, получателей информации и всех операций передачи, контролируемой межсетевым экраном информации к узлам информационной системы и от них;

– возможность обеспечения фильтрации для всех операций перемещения через межсетевые экраны информации к узлам информационной системы и от них;

– возможность осуществлять фильтрацию, основанную на следующих типах атрибутов безопасности субъектов: сетевой адрес узла отправителя; сетевой адрес узла получателя; и информации: сетевой протокол, который используется для взаимодействия;

– возможность явно разрешать информационный поток, базируясь на устанавливаемых администратором межсетевых экранах наборе правил фильтрации, основанном на идентифицированных атрибутах;

– возможность явно запрещать информационный поток, базируясь на устанавливаемых администратором межсетевых экранах наборе правил фильтрации, основанном на идентифицированных атрибутах;

– возможность блокирования всех информационных потоков, проходящих через нефункционирующий или функционирующий некорректно межсетевой экран;

– возможность регистрации и учета выполнения проверок информации сетевого трафика;

– возможность читать информацию из записей аудита уполномоченным администраторам;

– возможность выбора совокупности событий, подвергающихся аудиту, из совокупности событий, потенциально подвергаемых аудиту;

– возможность идентификации администратора межсетевым экраном до разрешения любого действия (по администрированию),

выполняемого при посредничестве межсетевого экрана от имени этого администратора;

– возможность аутентификации администратора межсетевым экраном до разрешения любого действия (по администрированию), выполняемого при посредничестве межсетевого экрана от имени этого администратора;

– поддержка определенных ролей по управлению межсетевым экраном;

– возможность со стороны администраторов управлять режимом выполнения функций безопасности межсетевого экрана;

– возможность со стороны администраторов управлять данными межсетевого экрана, используемыми функциями безопасности межсетевого экрана;

– возможность со стороны администраторов управлять атрибутами безопасности;

– возможность обеспечения перехода в режим аварийной поддержки, который предоставляет возможность возврата межсетевого экрана к штатному функционированию;

– возможность обеспечения надежных меток времени при проведении аудита безопасности.

В результате для сравнения были выбраны следующие межсетевые экраны.

– межсетевой экран Cisco ASA-SM1 с установленным программным обеспечением Cisco ASA версии 9.x;

– межсетевой экран Huawei Eudemon (модель Eudemon 8000E-X3) версии V500;

– межсетевой экран UserGate;

– межсетевой экран «Интернет Контроль Сервер (ИКС)»;

– межсетевой экран Ideco MX Cert.

Выбор критериев основывался на том, что важно для организации в вопросе сетевой безопасности и чаще всего востребовано в функциональном наполнении. В результате получились следующие группы критериев сравнения:

Общие сведения:

– компания;

– целевой сегмент:

– сертификаты;

– поддерживаемые языки интерфейса.

Архитектура

– поддерживаемые варианты исполнения;

– модули решения.

Функции межсетевого экранирования:

– статистическая трансляция сетевых адресов SNAT;

– динамическая трансляция сетевых адресов DNAT;

– политики контроля по зонам;

– политики контроля на основе интерфейсов.

Основные функции:

– система обнаружения / предотвращения вторжений (IDS/IPS);

– поддержка формирования исключений для сигнатур;

– поддержка уведомлений, отправка отчетов;

– противодействие известным методам обхода сигнатурного анализа;

– контроль приложений;

– контроль доступа (блокирование/разрешение, отслеживание) на основе распознаваемых сетевых приложений;

– возможность блокирования нераспознанных приложений;

– возможность контроля доступа по категориям / группам приложений;

– защита от DDos-атак;

– антивирусная защита (Anti-virus);

– антибот-защита (Anti-bot);

– защита почтового трафика (безопасность почты, антиспам) (входит проверка ссылок в теле письма, поддержка проверки вложенных файлов и архивов, поддерживаемые механизмы идентификации спама);

– веб-фильтрация (поддержка создания черных и белых список URL-адресов, поддержка фильтрации по репутации домена (IP), поддержка возможности блокировки по произвольному списку URL и IP);

– обнаружение утечек информации (DLP);

– анализ угроз (Threat Intelligence).

Дополнительные функции:

– поддерживаемые варианты управления (варианты консоли);

– поддержка управления доступом на основе ролей;

– автоматическое оповещение о событиях по электронной почте;

– поддержка возврата устройства на предыдущую конфигурацию, версию ПО;

– просмотр журналов (логов).

Далее производилось перечисление фактов о каждом из участвующих решений согласно критериям, которые указаны выше. Соответственно, брался определённый продукт в отдельности, анализировался по каждому параметру, после результаты сводились в единую таблицу (таблица 2).

Таблица 2 – Таблица сравнения межсетевых экранов

Параметр сравнения	Cisco	Huawei	Usergate	Ideco	Интернет Контроль Сервер (ИКС)
1	*2*	*3*	*4*	*5*	*6*
Общие сведения					
Компания	Cisco Systems Inc.	HUAWEI	UserGate / ООО "Юзергейт"	ООО «Айдеко»	ООО «А-Реал Консалтинг»
Целевой сегмент	Малый, средний и крупный бизнес, государственный и коммерческий сектор	Малый, средний и крупный бизнес, государственный и коммерческий сектор	Малый, средний и крупный бизнес, государственный и коммерческий сектор	Малый, средний и крупный бизнес, государственный сектор	Малый, средний и крупный бизнес, государственный сектор
Сертификаты	Сертификат ФСТЭК России №3973	Сертификат ФСТЭК №4083	Сертификат ФСТЭК №3905	Нет	Нет
Поддерживаемые языки интерфейса	Английский	Английский, китайский	Русский, английский	Русский	Русский, английский
Архитектура					
Поддерживаемые варианты исполнения	Аппаратное, виртуальное	Аппаратное, виртуальное, контейнерное	Аппаратное, виртуальное	Аппаратное, виртуальное	Аппаратное, виртуальное
Модули решения	МСЭ нового поколения, система обнаружения и предотвращения вторжений, защита от вредоносных программ, анализ угроз, фильтрация доступа к ресурсам сети Интернет и др	Firewall, URL Filtering, песочница, IPS, Anti-Bot, Anti-Virus, QoS, Monitoring, DLP, Anti-Spam, DDoS, Load-Balance, VPN, Application Control, Identity Firewall	Межсетевой экран, контентная фильтрация, VPN-сервер, IPS/IDPS, Антивирусная защита, защита почтового трафика, защита АСУ ТП, балансировщик, shaper, защита от	Антивирус Касперского, антиспам Касперского, контроль приложений, предотвращение вторжений, контент-фильтр	Межсетевой экран, IDS/IPS Suricata, Web Application Firewall, Anti-Virus, Anti-Spam, HTTPS-фильтрация, NAT, VLAN и DMZ, GRE / IPIP / OpenVPN-туннели с IPsec / PSK-шифрованием,

Продолжение таблицы 2

1	*2*	*3*	*4*	*5*	*6*
			DoS, Reverse proxy, web-портал (SSL VPN), контроль приложений L7; UserGate Log Analyzer - внешний сервер сбора и анализа журналов; UserGate Central Console - внешний сервер центрального управления удаленными устройствами UserGate.		утилита xauth, fail2ban, VPN, почтовый, файловый, FTP, прокси-, веб-, jabber-серверы, модуль IP-телефонии
Функции межсетевого экранирования					
Статистическая трансляция сетевых адресов SNAT	Да	Да	Да	Да	Да
Динамическая трансляция сетевых адресов DNAT	Да	Да	Да	Да	Да
Политики контроля по зонам	Да	Да	Да	Да	Нет
Политики контроля на основе интерфейсов	Да	Да	Нет	Да	Да
Основные функции					
Система обнаружения / предотвращения вторжений (IDS/IPS)	Да, модуль IPS/IDS	Да, модуль IPS/IDS	Да, модуль IPS с собственными сигнатурами	Да, IPS/IDS Suricata	Да, IPS/IDS Suricata

Продолжение таблицы 2

1	*2*	*3*	*4*	*5*	*6*
Поддержка формирования исключений для сигнатур	Да	Да	Да, через список правил, позволяющий указывать тип трафика для проверки и применяемый к нему профиль IPS/IDPS	Да	Нет
Поддержка уведомлений, отправка отчетов	Да	Да	Да	Да	Да
Противодействие известным методам обхода сигнатурного анализа	Да, препроцессоры обработки транспортных и прикладных протоколов, нормализация, декодирование и т.п.	Да, IDS Avoidance	Да, нормализация HTTP / HTTPS трафика. Возможность блокировки фрагментированных пакетов (включена по умолчанию), защита от VPN over DNS, блокирование туннелей Teredo, IP6-IP4, IP4-IP6	Нет	Нет
Контроль приложений	Да, модуль Cisco Application Visibility and Control	Да, модуль Huawei Smart Application Control	Да, модуль L7	Да, nDPI	Да, реализация на основе библиотеки nDPI

Продолжение таблицы 2

1	*2*	*3*	*4*	*5*	*6*
Контроль доступа (блокирование/разрешение, отслеживание) на основе распознаваемых сетевых приложений	Да, тысячи приложений и десятки тысяч микроприложений, возможность добавления своих приложений через OpenAppID	Да, более 6000 приложений	Да, определение приложений в транзитном трафике, блокирование известных приложений, блокирование всех неизвестных приложений	Да, 250 приложений	Да (все протоколы, распознаваемые nDPI)
Возможность блокирования нераспознанных приложений	Да	Да	Да	Нет	Нет
Возможность контроля доступа по категориям / группам приложений	Да	Да	Да	Нет	Нет
Защита от DDos-атак	Да, возможность установки модуля vDP Radware для Firepower 4100/9300	Да	Обнаружение и защита от SYN-, UDP-, ICMP-флуда, защита приложений от превышения сессий	Да (защита от SYN, ICMP, UDP-флуда, защита с помощью правил Suricata)	Да, на основе Suricata
Антивирусная защита (Anti-virus)	Да, Cisco AMP	Да, Huawei AV	Да, собственный и Kaspersky	Да, Kaspersky Antivirus	Да (ClamAV, Kaspersky Antivirus)
Антибот-защита (Anti-bot)	Да, Talos для всех модулей, включая AVC, IPS/IDS,	Да, через модуль IPS	Да, запрет доступа к известным командным серверам в	Да, модуль IPS	Нет

Продолжение таблицы 2

1	*2*	*3*	*4*	*5*	*6*
	фильтрацию HTTP/HTTPS, AMP		настройках межсетевого экранирования		
Защита почтового трафика (безопасность почты, антиспам) (входит проверка ссылок в теле письма, поддержка проверки вложенных файлов и архивов, поддерживаемые механизмы идентификации спама)	Нет	Да, модуль Mail Filtering	Да, модуль защиты почтового трафика	Да (модуль Kaspersky Anti-Spam)	Да (SpamAssassin, rspamd, Kaspersky Anti-Spam)
Веб-фильтрация (поддержка создания черных и белых список URL-адресов, поддержка фильтрации по репутации домена (IP), поддержка возможности блокировки по произвольному списку URL и IP)	Да, HTTP/HTTPS-фильтрация	Да, модуль URL Filtering	Да, модуль контентной фильтрации	Да, контент-фильтр	Да, контент-фильтрДа (SkyDNS, Kaspersky Web Filter)
Обнаружение утечек информации (DLP)	Нет	Да, модуль DLP	Да	Нет	Да
Анализ угроз (Threat Intelligence).	Да, Cisco Talos, поддержка внешних фидов по STIX/TAXII	Да, WeiRan Lab, поддержка внешних фидов	Да, модуль ATP (Advanced Threat Protection), наличие собственной базы Threat Intelligence	Нет	Нет

Продолжение таблицы 2

1	*2*	*3*	*4*	*5*	*6*
Дополнительные функции					
Поддерживаемые варианты управления (варианты консоли)	Централизованная система управления FMC, локальная система управления FDM, облако CDO, интерфейс командной строки	Централизованная система управления, SSH, netconf	Веб-консоль, CLI-консоль, API	SSH, веб-интерфейс	Веб-консоль, удалённая веб-консоль
Поддержка управления доступом на основе ролей	Да	Да	Да	Нет	Да
Автоматическое оповещение о событиях по электронной почте	Да	Да	Да	Нет	Да
Поддержка возврата устройства на предыдущую конфигурацию, версию ПО	Да	Нет	Да	Нет	Нет
Просмотр журналов (логов)	Да	Да	Да	Да	Да

Исходя из данных таблицы, по некоторым критериям не проходят межсетевые экраны Ideco и Интернет Контроль Сервер (ИКС), что подразумевает отсечение данных межсетевых экранов из сравнения.

Также из-за ухода компании Cisco из российского рынка не представляется возможным дальнейшее сравнение данного межсетевого экрана и дальнейшие рекомендации по его применению в образовательной организации.

В результате проводилась индивидуальная экспертная оценка межсетевых экранов Huawei и Usergate собственными силами.

Первым шагом определялся список потребностей, в отсортированном по приоритетности порядке. Для образовательной организации нужен такой межсетевой экран, который будет не дорогой в стоимости закупки и прост в установке и эксплуатации. Из-за возможных санкций предпочтительнее использовать продукт отечественного производителя. Немаловажную роль играет простота использования продукта и его функционал. В результате был разработан список с проставленными индексами значимости (от 1 до 9):

- простота установки – 9;
- стоимость закупки и эксплуатации – 9;
- импортозамещение – 7;
- простота использования – 5;
- оперативность реагирования – 3.

Вторым шагом определялись технические характеристики. Брались следующие критерии: архитектура решения, общая информация, функциональные особенности, интеграционные возможности, дополнительные критерии, соответствие направлению импортозамещения. Ориентируясь на доступные сведения о каждом продукте, заполнялись поля весовыми значениями от 0 до 9, а затем по итогам этой работы выставлялось среднее значение для каждой группы критериев (таблица 3).

Таблица 3 – Оценка межсетевых экранов по группам критериев

Критерий	Usergate	Huawei
1	*2*	*3*
Архитектура решения	4	3
Функциональные особенности	4	4
Соответствие направлению импортозамещения	4	2
Интеграционные возможности	3	4
Дополнительные критерии	4	4

Основными показателями является связь критерия и потребности:

Сильная связь – умножаем значение критерия на индекс значимости, разделенный на 100.

Средняя связь – умножаем значение критерия на индекс значимости, разделенный на 200.

При отсутствии связи между критерием и потребностью – проставляется 0.

Соотнесенные данные заполняются в таблицу оценки значимости критериев (таблица 4, 5).

Таблица 4 – Оценка значимости критериев для межсетевого экрана Usergate

Критерий	Простота установки (0,9)	Стоимость закупки и эксплуатации (0,9)	Импортозамещение (0,7)	Простота использования (0,5)	Оперативность реагирования (0,3)
Архитектура решения	3,6	3,6	0	2	0
Функциональные особенности	0	3,6	0	2	1,2
Соответствие направлению импортозамещения	0	0	2,8	0	0
Интеграционные возможности	2,7	2,7	2,1	1,5	0,9
Дополнительные критерии	3,6	3,6	2,8	0	0
Итого	9,9	13,5	7,7	5,5	2,1

Таблица 5 – Оценка значимости критериев для межсетевого экрана Huawei

Критерий	Простота установки (0,9)	Стоимость закупки и эксплуатации (0,9)	Импорт озамещение (0,7)	Простота использования (0,5)	Оперативность реагирования (0,3)
Архитектура решения	2,7	2,7	0	1,5	0
Функциональные особенности	0	3,6	0	2	1,2
Соответствие направлению импортозамещения	0	0	1,7	0	0
Интеграционные возможности	2,7	2,7	2,1	1,5	0,9
Дополнительные критерии	3,6	3,6	2,8	0	0
Итого	9	12,6	6,6	5	2,1

В результате сравнения с учётом определённых целей, стратегии образовательной организации и оценки критичности влияющих факторов, можно отдать предпочтение межсетевому экрану Usergate (таблица 6).

Таблица 6 – Результаты выбора

Usergate	Huawei
38,7	35,3

Оптимальным решением для образовательных организаций послужит межсетевой экран UserGate C100. Он является компактным и удобным в настройке сетевым устройством, способным обеспечить безопасность сетей небольших организаций или филиалов с числом пользователей от нескольких десятков до сотни и более. UserGate 100 предлагается по минимальным ценам, что делает его доступным для небольших организаций.

С помощью данного межсетевого экрана можно обеспечить не только базовую функциональность межсетевого экранирования, но и обеспечить защиту от современных атак, анализ и фильтрацию трафика по контенту, контроль интернет-приложений, блокирование опасных скриптов и приложений, защиту от вирусов и спама, а также другие функции безопасности.

Основные функции:

– межсетевой экран нового поколения;
– система обнаружения вторжений (IDS/IPS);
– доступ к внутренним ресурсам через SSL VPN Portal;
– анализ и выгрузка информации об инцидентах безопасности (SIEM);
– автоматизация реакции на угрозы безопасности информации (SOAR);
– обратный прокси;
– контроль доступа в интернет;
– контроль приложений L7;
– дешифрование SSL;
– гостевой портал;
– безопасная публикация внутренних ресурсов и сервисов;
– антивирусная защита;
– Advanced Threat Protection;
– безопасность почты;
– идентификация пользователей;
– поддержка концепции BYOD (Bring Your Own Device);
– виртуальная частная сеть (VPN);
– удаленное администрирование;
– поддержка АСУ ТП (SCADA);
– поддержка кластеризации и высокой отказоустойчивости [23].

Таким образом корпоративную информационную систему образовательной организации нужно защищать в обязательном порядке. Межсетевой экран уменьшит вероятность вторжения извне, позволит установить ограничения на использование определенных программ сотрудниками, обеспечит безопасную передачу данных по FTP и прочим протоколам. Применение сертифицированного межсетевого экрана

рекомендуется образовательным учреждениям, для которых важно отслеживать работу персонала и не допускать использование «непрофильных» программ и сайтов. При этом лучше установить аппаратно-программный брандмауэр, чтобы дополнительно не нагружать рабочие компьютеры.

2.3 Разработка обучающего курса по применению средств защиты корпоративной информационной системы образовательной организации

Для реализации защиты корпоративной информационной системы важно проводить обучение и тренировки по вопросам информационной безопасности. В соответствии с разработанными рекомендациями для ГБПОУ «Южно-Уральского государственного технического колледжа» был выбран межсетевой экран UserGate, как комплексное средство защиты корпоративной информационной системы образовательной организации.

Исходя из выбора, был разработан обучающий курс на тему «Администрирование межсетевого экрана UserGate», который является вводным для базового ознакомления с конфигурацией и эксплуатацией межсетевого экрана UserGate.

Курс предназначен для системных администраторов и может быть внедрён в образовательный процесс в виде дополнительной общеобразовательной программы для специальности 09.02.06 Сетевое и системное администрирование. В рамках обучающего курса для ознакомления будущих специалистов с межсетевыми экранами UserGate была выбрана версия 2.8, так как данная версия является стабильной и простой в настройке.

Курс состоит из 7 лекций, 6 тестов, 3 практических работ.

Программа курса:

1. *Введение в многофункциональные сетевые экраны.* Требования к современным межсетевым экранам. Типы межсетевых экранов. Варианты размещения межсетевых экранов в корпоративной сети. Краткий обзор ключевых возможностей межсетевого экрана UserGate.

Практическая работа 1. Настройка прокси-сервера.

2. *Управление учетными записями пользователей*. Способы хранения информации о пользователях. Способы идентификации пользователей.

Практическая работа 2. Настройка клиентской станции.

3. *Маршрутизация и фильтрация трафика.* Правила фильтрации.

Практическая работа 3. Мониторинг трафика.

После окончания курса будущие специалисты научаться:

– настраивать прокси-сервер: создание группы пользователей, ограничения для групп пользователей, расстановка защиты от несанкционированного доступа;

– настраивать клиентскую станцию: проверка IP, включение параметра прокси-сервера, проверка работы фильтров;

– просматривать объемы отправленной и полученной информации клиентом, отслеживать посещаемые ресурсы, осуществлять мониторинг истории просмотренных ресурсов.

Предварительно разработанные материалы для теоретического изучения, контроля знаний и практических работ переносятся в российскую образовательную платформу и конструктор бесплатных и платных открытых онлайн-курсов и уроков Stepik [54].

Данный ресурс позволяет любому зарегистрированному пользователю создавать интерактивные обучающие уроки и онлайн-курсы, используя видео, тексты и разнообразные задачи с автоматической проверкой и моментальной обратной связью. В процессе обучения студенты могут вести обсуждения между собой и задавать вопросы преподавателю на форуме.

Курсы на платформе состоят из уроков, сгруппированных в тематические модули, однако уроки могут существовать отдельно и собираются в библиотеку на платформе. Уроки состоят из шагов, которые могут представлять собой текст, видео-лекцию или практическое задание. На платформе можно использовать 20 типов заданий, включая тесты, числовые

задачи, задания с математическими формулами и химическими уравнениями, пазлы, задачи на программирование.

Создатели курсов сохраняют за собой авторские права, могут без ограничений использовать созданные материалы в виде курсов или отдельных уроков, хранить их для самостоятельной подготовки студентов, встраивать на другие сайты и образовательные платформы, следить за статистикой и прогрессом студентов. Все курсы и материалы, размещенные на Stepik, лицензируются для свободного использования на условиях лицензии Creative Commons Attribution-ShareAlike 4.0.

Существуют также годовые и короткие онлайн-программы. В зависимости от договорённости с вузом, слушателям по результатам могут выдаваться дипломы о профессиональной переподготовке.

Для того, чтобы курс был опубликован, необходимо выполнить ряд условий, которые отображаются во вкладке Чек-лист (рисунок 6).

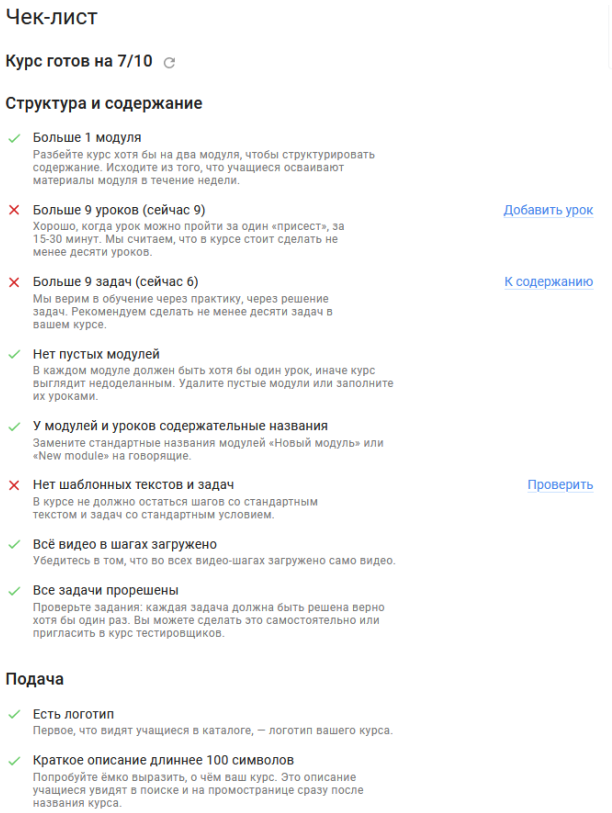


Рисунок 6 – Требования, предъявляемые Stepik для публикации своего курса

Как только все условия будут выполнены – курс может быть опубликован на платформе для дальнейшего прохождения студентами. (рисунок 7, рисунок 8)

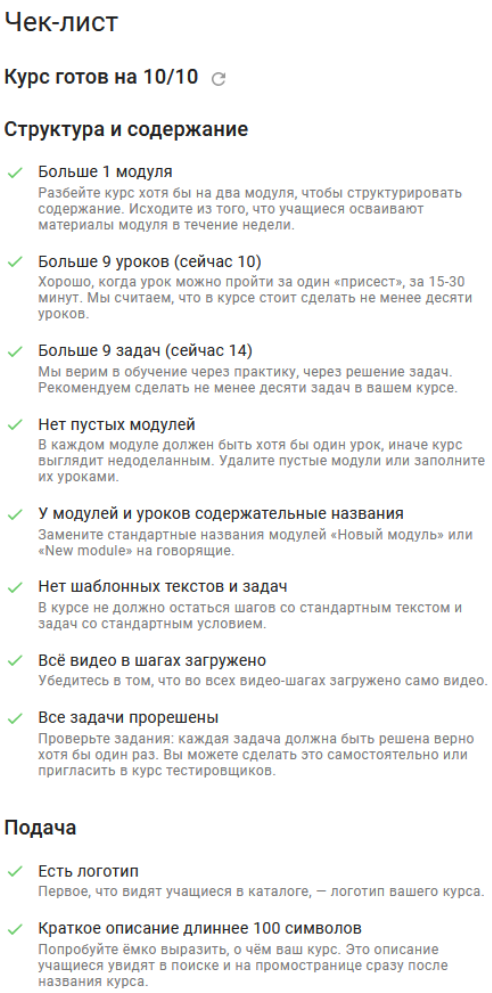


Рисунок 7 –Выполненные требования предъявляемые Stepik для публикации своего курса

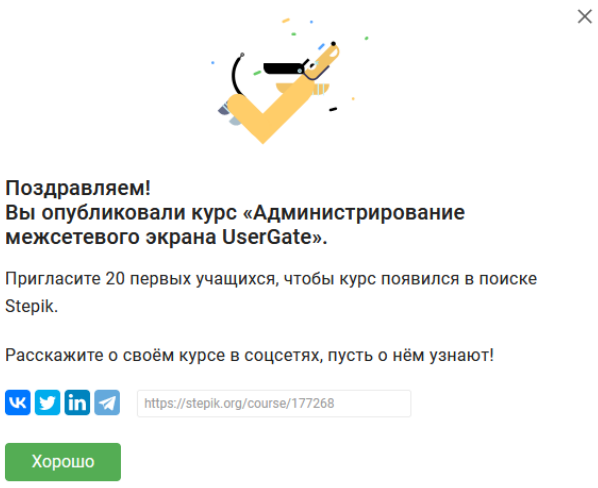


Рисунок 8 – Окно с подтверждением опубликования курса

Для того, чтобы начать прохождение курса студенту необходимо войти (рисунок 9) или зарегистрироваться (рисунок 10) на Stepik.

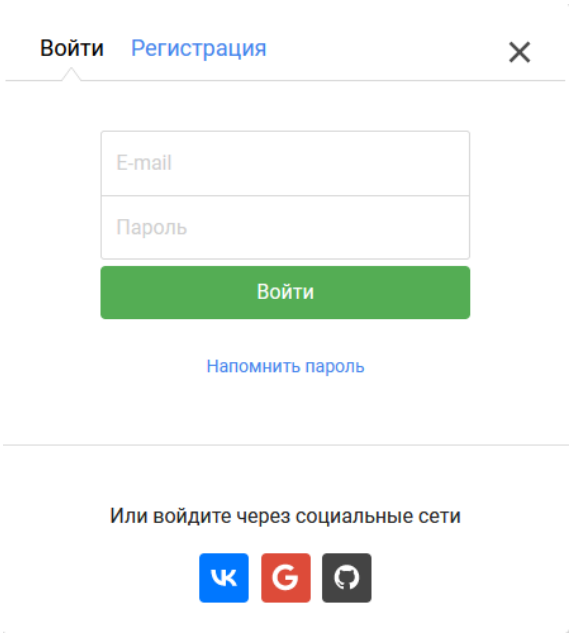


Рисунок 9 – Окно входа Stepik

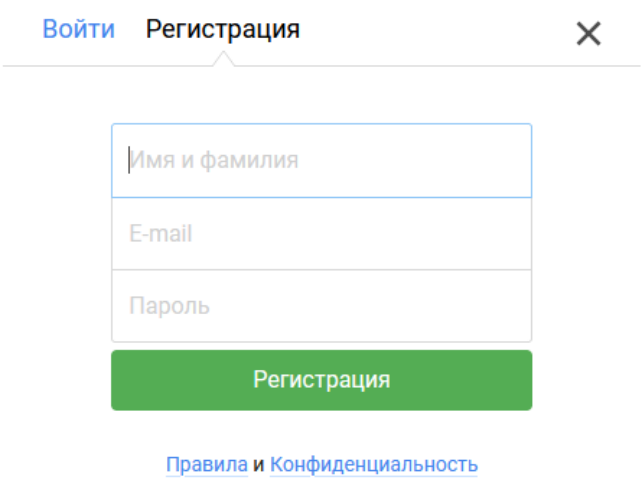


Рисунок 10 –Окно регистрации Stepik

Далее в окне поиска найти курс «Администрирование межсетевого экрана UserGate» или пройти по ссылке, которую выдаёт преподаватель: https://stepik.org/course/177268.

Студент попадёт на окно с курсом, где можно просмотреть его название, краткое описание, уровень для обучения, рекомендуемую нагрузку в неделю, чему научится студент после прохождения курса, для кого предназначен этот курс, как будет проходить обучение (рисунок 11).

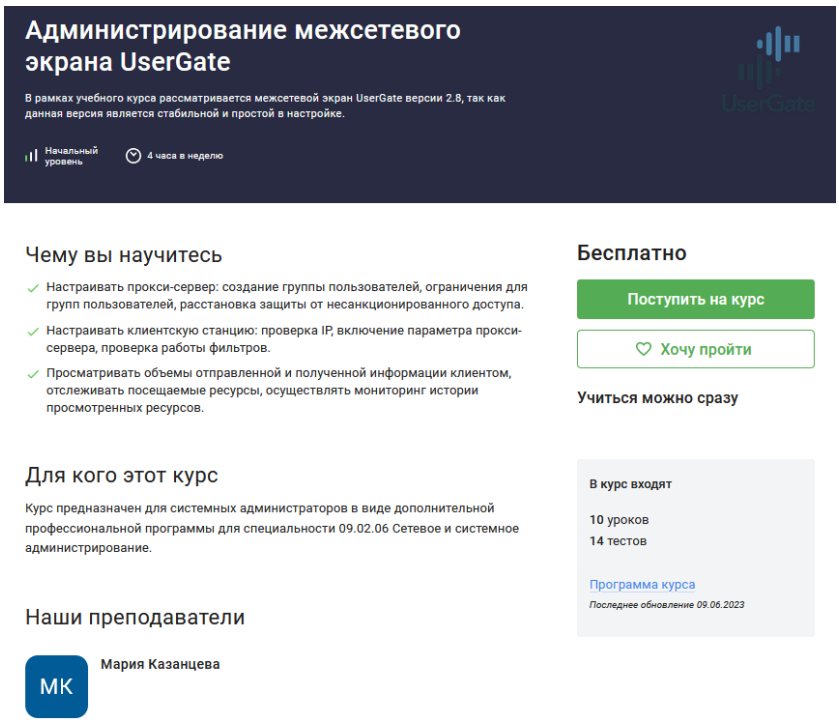


Рисунок 11 – Главная страница курса «Администрирование межсетевого экрана UserGate»

Ниже обучающийся может просмотреть программу курса, его цену, поступить на курс и добавить его в избранное (рисунок 12).

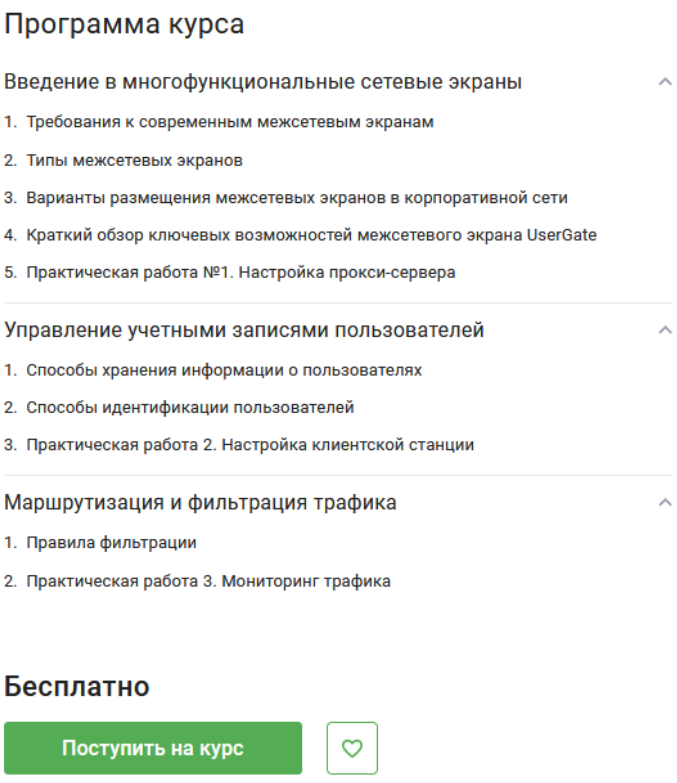


Рисунок 12 – Программа курса, его цена и кнопка для поступления на курс

После нажатия на кнопку «Поступить на курс» курс добавляется во вкладку «Моё обучение», где можно с лёгкостью вернуться обратно к обучению курса и просмотреть статистику его прохождения (рисунок 13).

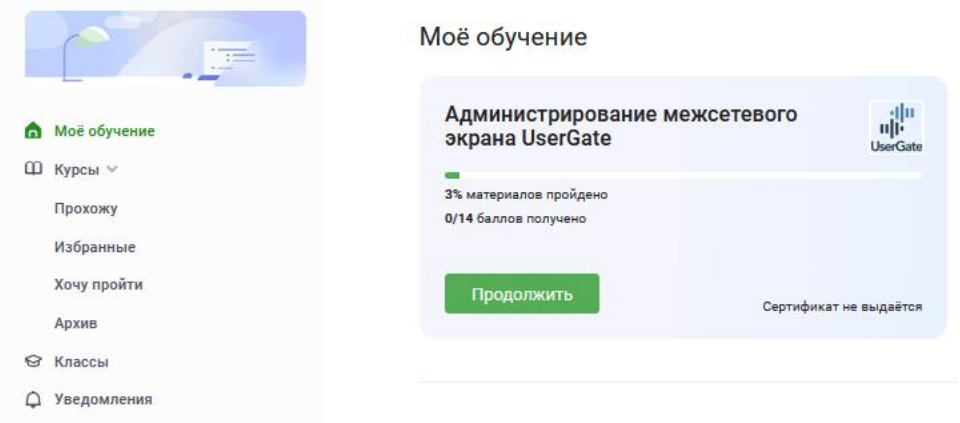


Рисунок 13 – Вкладка «Моё обучение» с курсами, который студент проходит на данный момент

При нажатии на кнопку «Продолжить» студент переходит на страницу с первой темой курса, где ему необходимо прочитать лекционный материал и законспектировать его в тетрадь для дальнейшей проверки преподавателем (рисунок 14).

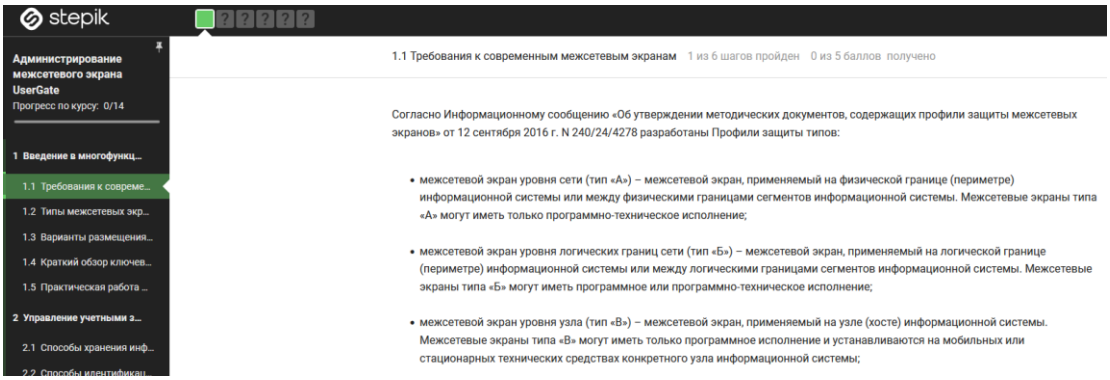


Рисунок 14 – Вид лекционного материала

Для перехода на следующий шаг, обучающийся должен нажать на кнопку «Следующий шаг» (рисунок 15).

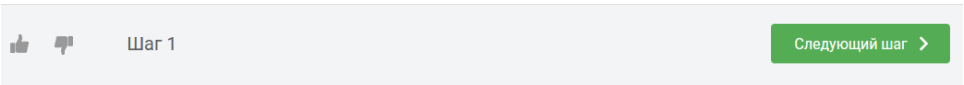


Рисунок 15 – Кнопка «Следующий шаг»

После лекционного материала студенту необходимо пройти тестирование для закрепления полученных знаний. В рамках курса

используются тесты: на выбор одного правильного ответа, на выбор нескольких правильных ответов, на классификацию, на свободный ответ, на подстановку.

На рисунке 16 представлен вопрос на различение с выбором одного правильного ответа.

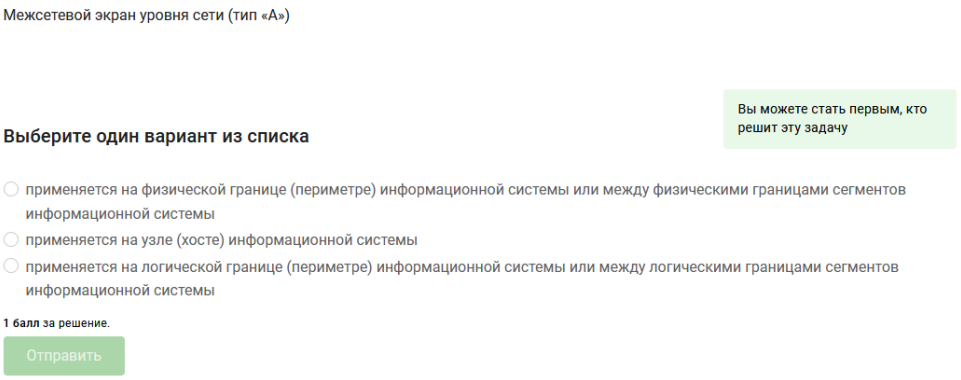


Рисунок 16–Вопрос на различение с выбором одного правильного ответа

На рисунке 17 представлен вопрос на различение с выбором нескольких правильных ответов.

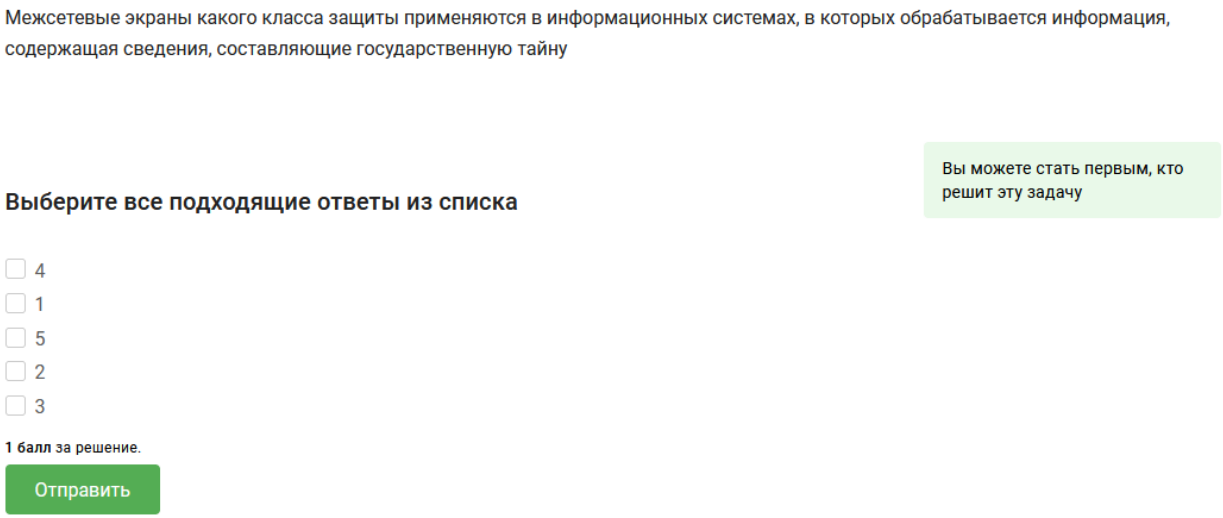


Рисунок 17 – Вопрос на различение с выбором нескольких правильных ответов

На рисунке 18 представлен вопрос на классификацию.

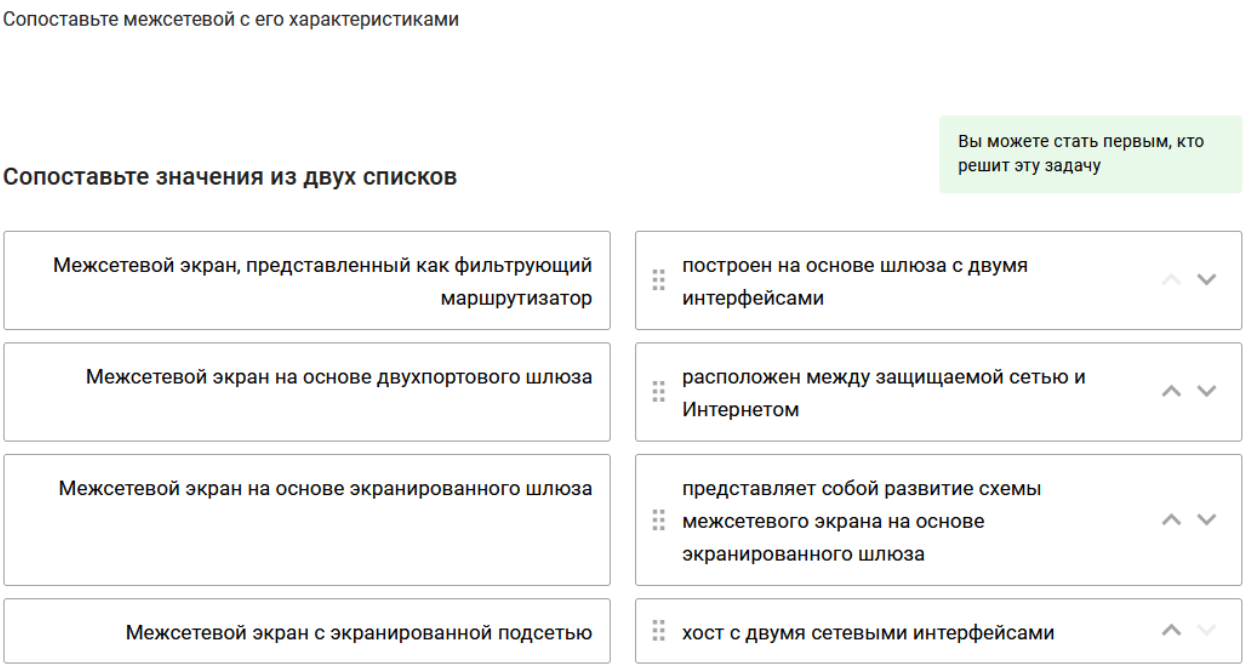


Рисунок 18 – Вопрос на классификацию

На рисунке 19 представлен вопрос на свободный ответ.

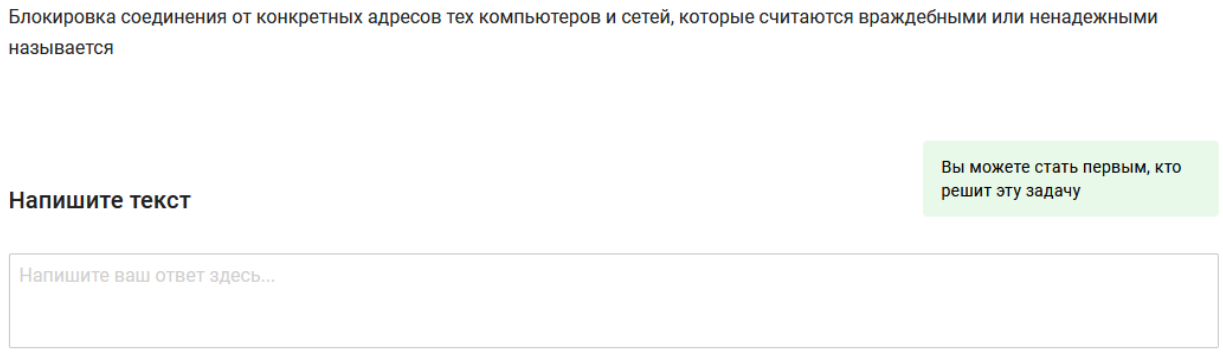


Рисунок 19 – Вопрос на свободный ответ

На рисунке 20 представлен вопрос на подстановку.

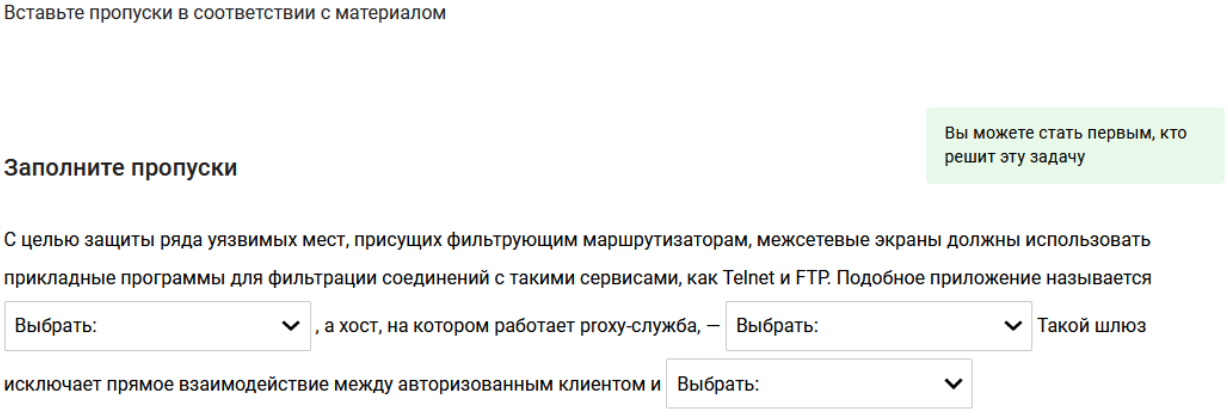


Рисунок 20 – Вопрос на подстановку

В конце каждого тематического модуля по курсу обучающемуся необходимо выполнить практическую работу для проверки полученных знаний на практике.

Для каждой практической работы необходимо выполнить отчёт, требования к которому располагаются перед выполнением работы (рисунок 21).

Требования к отчёту по практической работе

1. Отчёт выполнять в текстовом процессоре Microsoft Word.

2. Вначале пишется **номер практической работы и её название** (Пример: Практическая работа №1. Настройка прокси-сервера).

- Выравнивание заголовка по центру.
- Начертание - полужирное.
- Отступ - нет.
- Междустрочный интервал - 1,5.

3. Далее пишется **цель практической работы.**

- Выравнивание по ширине.
- Начертание - обычное.
- Отступ - 1,25.
- Междустрочный интервал - 1,5.

4. Далее **задания нумеруются** и **вставляются скриншоты полученного результата.**

для изображений

- Выравнивание по центру.
- Отступ - нет.
- Междустрочный интервал - 1,5.

для текста

- Выравнивание по ширине.
- Начертание - обычное.
- Отступ - 1,25.
- Междустрочный интервал - 1,5.

5. В конце пишется **вывод**: по цели в прошедшем времени (Пример: научилась выполнять..., освоила навыки...)

Рисунок 21 – Требования к отчёту по практической работе

Нажимая кнопку «Следующий шаг» студент попадает на страницу с заданиями к практической работе (рисунок 22).

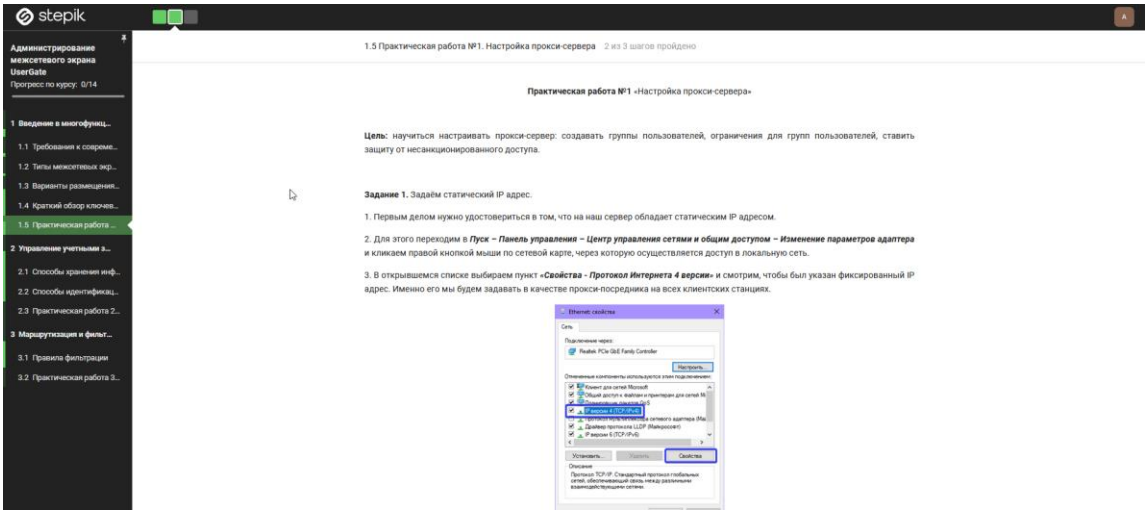


Рисунок 22 – Вид практической работы

После выполнения практической работы и создания отчёта, его необходимо направить на почту преподавателя для дальнейшей проверки (рисунок 23).

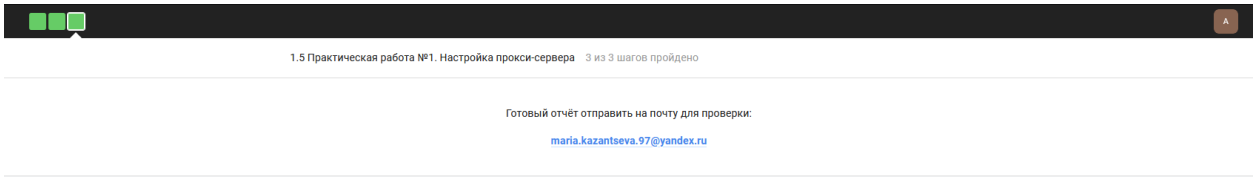


Рисунок 23 – Отправка отчёта на почту преподавателя

После прохождения курса откроется окно с подтверждением прохождения курса (рисунок 24).

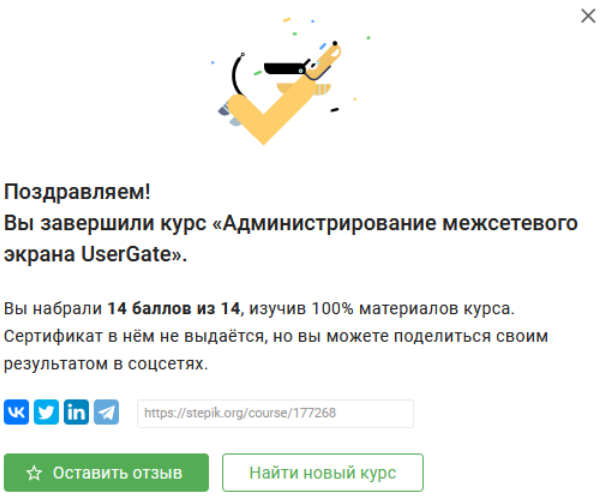


Рисунок 24 – Окно завершения курса

На рисунке 25 представлено отображение пройденного курса на вкладке «Моё обучение».

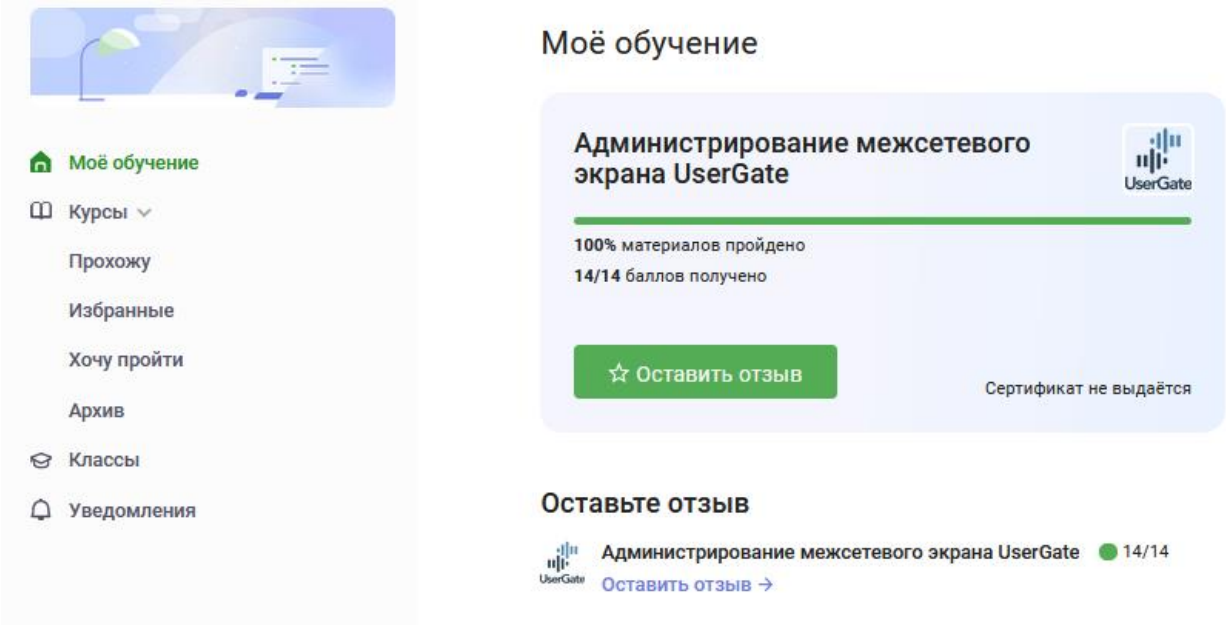


Рисунок 25 – Пройденный курс на вкладке «Моё обучение»

Разработанный учебный курс является одним из инструментов осуществления и одним из средств реализации защиты корпоративной информационной системы.

Задания, выполняемые каждым обучающимся, позволяют отслеживать усвоение, закрепление и применение знаний по пройденному материалу на практике, что даёт возможность студентам быстро и качественно восстановить пройденный материал, применять его в дальнейшей профессиональной деятельности в сфере обслуживания межсетевых экранов.

2.4 Оценка эффективности рекомендаций по выбору средств защиты корпоративной информационной системы образовательной организации ГБПОУ «Южно-Уральский государственный технический колледж»

В комплекс рекомендаций по выбору средств защиты корпоративной информационной системы входили анализ нормативно-правовых требований действующего законодательства и анализ угроз образовательной организации. В результате были разработаны рекомендации по выбору средств межсетевого экранирования, в которые вошли ряд критериев, учитывающие специфику и

цели образовательной организации, а также экспертная оценка, которая позволяет выбрать оптимальный межсетевой экран для образовательной организации. Также в комплекс рекомендаций по защите корпоративной информационной системы вошло обучение будущих специалистов в данной области на обучающем курсе по теме ««Администрирование межсетевого экрана UserGate».

В результате была произведена экономическая оценка эффективности рекомендаций по выбору средств защиты корпоративной информационной системы образовательной организации ГБПОУ «Южно-Уральский государственный технический колледж».

В экономическую оценку вошли:

1. Обследование информационных систем.
2. Обучение.
3. Перспективы внедрения межсетевого экранирования в образовательную организацию.

В обследование информационных систем входило:

– аудит документов, обследование помещений, сети и компьютеров;
– разработка модели угроз.

Учебный курс может быть внедрён в образовательный процесс в виде дополнительной образовательной общеразвивающей программы, оплата которой будет соответствовать почасовой. На данный момент ставка составляет в среднем 150 руб./ч. Одна лекция и одно практическое занятие по учебному расписанию составляет 1 час 90 минут (округляется до 2 часов). Исходя из того, что в программу курса входит 7 лекций и 3 практических занятия, можно сделать вывод, что преподаватель за весь курс обучения должен получить зарплату в 3 000 руб на одну учебную группу.

Сеть образовательной организации должна быть защищена от внешних атак, вирусов и разнообразных современных киберугроз. Межсетевой экран UserGate является экономически выгодным решением для образовательной организации, как в плане защиты, так и в плане ценообразования.

Согласно прайс-листу цена на UserGate C100, который подходит для малого бизнеса, филиалов, POS-систем, школ/колледжей, Wi-Fi точек на 2023 год составит за 1 год – 155 500 руб., за 3 года – 214 320 руб (таблица 7).

Данное устройство поставляется практически готовым к использованию, и его настройка может быть произведена обычным системным администратором.

Таблица 7 – Прайс-лист на UserGate C100

Позиция	Стоимость за 1 год, руб.	Стоимость за 3 года, руб.	Примечание
Аппаратная платформа UserGate C	69000	69000	Цена с НДС 18%
Приобретение права на использование UserGate для модели C100	86500		НДС не облагается
Приобретение права на использование UserGate + Подписка Security Updates (2 года) для модели C100		145320	НДС не облагается

В результате была составлена таблица расчёта стоимости защиты корпоративной информационной системы образовательной организации (таблица 8).

Таблица 8 – Расчёт стоимости защиты корпоративной информационной системы образовательной организации

№	Наименование товаров и услуг	Цена, руб.	Количество	Стоимость, руб.
1	*2*	*3*	*4*	*5*
I	ОБСЛЕДОВАНИЕ ИНФОРМАЦИОННЫХ СИСТЕМ			
1.1	Проведение обследования (аудит документов, обследование помещений, сети и компьютеров)	4 000	1	4 000
1.2	Разработка модели угроз	5 450	1	5 450
II	ОБУЧЕНИЕ	3 000	3	9 000
				18 450
III	ВНЕДРЕНИЕ МЕЖСЕТЕВОГО ЭКРАНИРОВАНИЯ В ОБРАЗОВАТЕЛЬНУЮ ОРГАНИЗАЦИЮ			
3.1	Аппаратная платформа UserGate C	69 000	1	69 000
3.2	Приобретение права на использование UserGate + Подписка Security Updates (2 года) для модели C100	145 320	1	145 320
IV	ОПЛАТА СИСТЕМНОГО АДМИНИСТРАТОРА			

Продолжение таблицы 8

1	*2*	*3*	*4*	*5*
4.1	Настройка, управление и мониторинг межсетевого экрана UserGate C100	27 000	*входит в ежемесячную оплату труда*	27 000
				241 320

В случае выявления нарушения в области информационной безопасности образовательной организации предусмотрена уголовная, административная, дисциплинарная и гражданская ответственность (таблица 9), которая может применяться в отношении организации, руководителя организации, подразделения или виновного работника [29].

Таблица 9 – Нарушения в области информационной безопасности и соответствующие им штрафы

Уголовная ответственность		
Статья 137 УК РФ. Нарушение неприкосновенности частной жизни	Незаконное собирание или распространение сведений о частной жизни лица, составляющих его личную или семейную тайну, без его согласия либо распространение этих сведений в публичном выступлении, публично демонстрирующемся произведении или средствах массовой информации	наказываются штрафом в размере до двухсот тысяч рублей или в размере заработной платы или иного дохода осужденного за период до восемнадцати месяцев
Статья 272 УК РФ. Неправомерный доступ к компьютерной информации	Неправомерный доступ к охраняемой законом компьютерной информации, если это деяние повлекло уничтожение, блокирование, модификацию либо копирование компьютерной информации	наказывается штрафом в размере до двухсот тысяч рублей или в размере заработной платы или иного дохода осужденного за период до восемнадцати месяцев
Статья 274 УК РФ. Нарушение правил эксплуатации средств хранения, обработки или передачи компьютерной	Нарушение правил эксплуатации средств хранения, обработки или передачи охраняемой компьютерной информации либо	наказывается штрафом в размере до пятисот тысяч рублей или в размере заработной платы или иного дохода осужденного за период до восемнадцати месяцев

Продолжение таблицы 9

информации и информационно-телекоммуникационных сетей	информационно-телекоммуникационных сетей и оконечного оборудования, а также правил доступа к информационно-телекоммуникационным сетям, повлекшее уничтожение, блокирование, модификацию либо копирование компьютерной информации, причинившее крупный ущерб	
Административная ответственность		
Статья 13.11 КоАП. Нарушение законодательства Российской Федерации в области персональных данных	Обработка персональных данных в случаях, не предусмотренных законодательством Российской Федерации в области персональных данных, либо обработка персональных данных, несовместимая с целями сбора персональных данных	влечет наложение административного штрафа на граждан в размере от двух тысяч до шести тысяч рублей; на должностных лиц - от десяти тысяч до двадцати тысяч рублей; на юридических лиц - от шестидесяти тысяч до ста тысяч рублей
Статья 13.12 КоАП. Нарушение правил защиты информации	Нарушение условий, предусмотренных лицензией на осуществление деятельности в области защиты информации	влечет наложение административного штрафа на граждан в размере от одной тысячи до одной тысячи пятисот рублей; на должностных лиц - от одной тысячи пятисот до двух тысяч пятисот рублей; на юридических лиц - от пятнадцати тысяч до двадцати тысяч рублей.
	Использование несертифицированных информационных систем, баз и банков данных, а также несертифицированных средств защиты информации, если они подлежат обязательной сертификации	влечет наложение административного штрафа на граждан в размере от одной тысячи пятисот до двух тысяч пятисот рублей с конфискацией несертифицированных средств защиты информации или без таковой; на должностных лиц - от двух тысяч пятисот до трех тысяч рублей; на юридических лиц - от двадцати тысяч до двадцати пяти тысяч рублей с конфискацией несертифицированных средств

Продолжение таблицы 9

		защиты информации или без таковой
Статья 13.13 КоАП. Незаконная деятельность в области защиты информации	Занятие видами деятельности в области защиты информации (за исключением информации, составляющей государственную тайну) без получения в установленном порядке специального разрешения (лицензии), если такое разрешение (такая лицензия) в соответствии с федеральным законом обязательно (обязательна)	влечет наложение административного штрафа на граждан в размере от пятисот до одной тысячи рублей с конфискацией средств защиты информации или без таковой; на должностных лиц - от двух тысяч до трех тысяч рублей с конфискацией средств защиты информации или без таковой; на юридических лиц - от десяти тысяч до двадцати тысяч рублей с конфискацией средств защиты информации или без таковой
Статья 13.14 КоАП. Разглашение информации с ограниченным доступом	Разглашение информации, доступ к которой ограничен федеральным законом (за исключением случаев, если разглашение такой информации влечет уголовную ответственность), лицом, получившим доступ к такой информации в связи с исполнением служебных или профессиональных обязанностей	влечет наложение административного штрафа на граждан в размере от пяти тысяч до десяти тысяч рублей; на должностных лиц - от сорока тысяч до пятидесяти тысяч рублей или дисквалификацию на срок до трех лет; на юридических лиц - от ста тысяч до двухсот тысяч рублей
Дисциплинарная ответственность		
Статья 90 ТК РФ	Ответственность за нарушение норм, регулирующих обработку и защиту персональных данных работника	
Статья 192 ТК РФ	Дисциплинарные взыскания	
за совершение дисциплинарного проступка работодатель имеет право применить дисциплинарные взыскания: замечание, выговор, увольнение по соответствующим основаниям.		

Согласно ФЗ РФ «Об образовании в Российской Федерации» всякое образовательное учреждение (учреждение, осуществляющее образовательный процесс) является юридическим лицом [34].

Таким образом максимальный штраф, который может получить образовательная организация за нарушения в области информационной безопасности составит 370 000 руб. Дополнительно возможна конфискация

средств защиты, приостановление или прекращение обработки персональных данных.

После выявления нарушений выписывается предписание с указанием сроков и необходимых мер по устранению. По наступлению указанных в предписании сроков по выполнению требований, будет произведена проверка на их исполнение. В случае отрицательного результата, будут повторно применены санкции и выписано очередное предписание.

Для расчета экономической эффективности разработанных рекомендаций выбора средств защиты корпоративной информационной системы необходимо суммарную её стоимость сравнить со стоимостью возможного ущерба со стороны регуляторных рисков (рисунок 26).

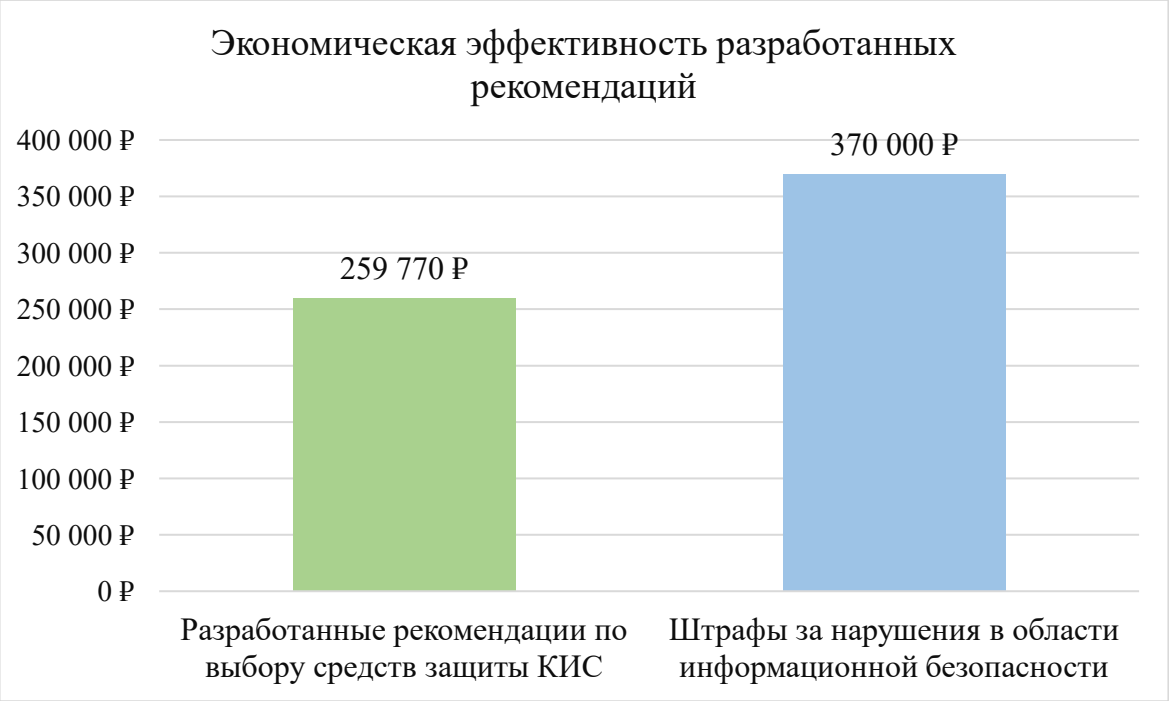


Рисунок 26 – Экономическая эффективность разработанных рекомендаций

В результате сравнения экономическая эффективность разработанных рекомендаций составила 110 230 руб. Учитывая данный показатель, можно сделать вывод, что реализация данного проекта экономически эффективна.

Таким образом, разработка рекомендаций по выбору средств защиты корпоративной информационной системы образовательной организации возможна при тщательном учёте всех аспектов, включая количественную оценку безопасности и размера ожидаемых потерь.

Вывод по второй главе

Во второй главе были разработаны рекомендации по выбору средств защиты корпоративной информационной системы образовательной организации, разработан обучающий курс по применению средств защиты корпоративной информационной системы образовательной организации, проведена оценка эффективности разработанных рекомендаций по выбору средств защиты корпоративной информационной системы образовательной организации.

Состав корпоративной информационной системы ГПБОУ «ЮУрГТК» разнороден. В нее входят: система для управления образовательным процессом и обеспечения коммуникации между преподавателями и студентами; система электронного документооборота; система электронного расписания; система электронной почты; система дистанционного обучения; система управления базами данных; система электронной библиотеки.

Целостность данных информационных систем подвержена различным угрозам, которые обусловлены действиями субъекта, техническими средствами и стихийными источниками. Угрозы проявляются через уязвимости, которые могут присутствовать в программах или аппаратных компонентах рабочих станций пользователей, а также в коммуникационном оборудовании и каналах связи информационной системы. Устранение или существенное ослабление уязвимостей влияет на возможность реализации угроз безопасности информации.

Для разработки рекомендаций было проанализировано текущее состояние системы защиты корпоративной информационной системы образовательной организации ГБПОУ «ЮУрГТК» с помощью модели угроз, в результате которого было выявлено, что корпоративная информационная система данной организации имеет объективные, субъективные и случайные уязвимости. Она может быть подвержена пассивным и активным атакам, к

последним относятся Backdoor, фишинг, переадресация маршрутов, взлом удалённого доступа, DoS-атака.

Определяя средства защиты корпоративной информационной системы образовательной организации, мы остановили свой выбор на межсетевых экранах, как комплексных средств защиты от угроз.

В разработанных рекомендациях представлена таблица сравнения межсетевых экранов, которая состоит из критериев, выбранных на основании важных для организации вопросов сетевой безопасности и чаще всего востребованного функционала в наполнении средств защиты. В критерии вошли следующие группы: общие сведения, архитектура, функции межсетевого экранирования, основные функции, дополнительные функции. Согласно критериям, проводилось перечисление фактов о каждом выбранном межсетевом экране. Если межсетевой экран не проходил по одному или нескольким критериям, он отсекался из сравнения.

В результате проводилась индивидуальная экспертная оценка межсетевых экранов собственными силами, в результате которой было отдано предпочтение межсетевому экрану UserGate, в частности – UserGate C100, так как он является оптимальным решением для образовательных организаций в силу своей компактности, удобством настройки и минимальной цены.

Так как в комплекс защиты корпоративной информационной системы входит проведение обучения и тренировок по вопросам информационной безопасности, был разработан обучающий курс «Администрирование межсетевого экрана», который предназначен для системных администраторов, но может быть использован в образовательном процессе в виде дополнительной общеобразовательной программы для специальности 09.02.06 Сетевое и системное администрирование.

Данный курс разработан на российской образовательной платформе и конструкторе бесплатных и платных открытых онлайн-курсов Stepik. Для доступа к курсу необходимо зарегистрироваться на сайте и найти его в поле поиска, либо по ссылке, которую выдаёт преподаватель.

В обучающий курс вошли лекционный материал; различные варианты тестовых заданий: на различение с одним и несколькими вариантами ответа, на классификацию, на свободный ответ, на подстановку; практические задания, направленные на самостоятельное выполнение их студентами. В результате изучения каждой темы происходит контроль знаний и проверка применения знаний на практике.

В итоге была проведена экономическая оценка эффективности рекомендаций по выбору средств защиты корпоративной информационной системы образовательной организации ГБПОУ «ЮУрГТК». В данную оценку вошли расчет стоимости внедрения межсетевого экранирования для защиты корпоративной информационной системы образовательной организации и стоимостью возможного ущерба со стороны регуляторных рисков.

На внедрение разработанных рекомендаций образовательная организация потратит 259770 рублей, а стоимость возможного ущерба за нарушения в области информационной безопасности составят 370 00- рублей. В результате сравнения данных показателей экономическая эффективность разработанных рекомендаций составила 110 230 рублей.

Учитывая данный показатель, можно сделать вывод, что реализация данного проекта экономически эффективна.

ЗАКЛЮЧЕНИЕ

Одним из актуальных на текущий момент вопросом в области защиты является защита корпоративных информационных систем образовательной организации в соответствии с российским законодательством и актуальными угрозами безопасности. От успешного функционирования данных систем зависит эффективность образовательных организаций, так как они предназначены для автоматизации всего комплекса управленческий задач, а именно: сбор и анализ информации, планирование, организация и координация действий, контроль над исполнением, внутренняя и внешняя коммуникация и т.д.

Грамотное обеспечение защиты корпоративной информационной системы должно быть комплексным. На это влияет постоянное расширение функциональности корпоративных информационных систем, нарастание зависимости от информационной инфраструктуры и угроза уничтожения, изменения, блокирования, копирования, предоставления, распространения информации посредством несанкционированного доступа. Для защиты должны применяться средства, прошедшие оценку соответствия в форме обязательной сертификации. К тому же, специфика защиты корпоративных информационных систем подразумевает хранение в них больших массивов персональных данных, обработка, хранение и передача которых должна осуществляться в соответствии с нормативными регулятивами.

В этой связи стала актуальна тема исследования: «Выбор средств защиты корпоративной информационной системы образовательной организации».

В работе была поставлена цель исследования: обосновать и разработать рекомендации по выбору средств защиты корпоративной информационной системы образовательной организации.

В ходе выполнения магистерской диссертации были изучены научно-методические основы корпоративной информационной системы и значение её

защиты в образовательной организации. Были изучены нормативно-правовые требования к выбору средств защиты корпоративной информационной системы образовательной организации. Были выявлены виды средств защиты корпоративной информационной системы образовательной организации.

В процессе исследования проанализировано текущее состояние системы защиты корпоративной информационной системы образовательной организации ГБПОУ «ЮУрГТК» и разработаны рекомендации по выбору средств защиты корпоративной информационной системы на примере данной образовательной организации.

В результате анализа было выявлено, что корпоративная информационная система ГБПОУ «ЮУрГТК» имеет объективные, субъективные и случайные уязвимости. Она может быть подвержена пассивным и активным атакам, к последним относятся Backdoor, фишинг, переадресация маршрутов, взлом удалённого доступа, DoS-атака.

Наиболее оптимальным средством защиты корпоративной информационной системы для ГБПОУ «ЮУрГТК» является межсетевой экран за счёт его разнообразных функциональных возможностей.

В разработанных рекомендациях представлена таблица сравнения межсетевых экранов, которая состоит из критериев, выбранных на основании важных для организации вопросов сетевой безопасности и чаще всего востребованного функционала в наполнении средств защиты. В критерии вошли следующие группы: общие сведения, архитектура, функции межсетевого экранирования, основные функции, дополнительные функции. Согласно критериям, проводилось перечисление фактов о каждом выбранном межсетевом экране. Если межсетевой экран не проходил по одному или нескольким критериям, он отсекался из сравнения.

В результате проводилась индивидуальная экспертная оценка межсетевых экранов собственными силами, в результате которой было отдано предпочтение межсетевому экрану UserGate, в частности – UserGate C100, так

как он является оптимальным решением для образовательных организаций в силу своей компактности, удобством настройки и минимальной цены.

Внедрение межсетевого экранирования UserGate C100 целесообразно сопроводить обучающим курсом «Администрирование межсетевого экрана», который предназначен для системных администраторов, но может быть использован в образовательном процессе в виде дополнительной общеобразовательной программы для специальности 09.02.06 Сетевое и системное администрирование. В обучающий курс вошли лекционный материал; различные варианты тестовых заданий: на различение с одним и несколькими вариантами ответа, на классификацию, на свободный ответ, на подстановку; практические задания, направленные на самостоятельное выполнение их студентами. В результате изучения каждой темы происходит контроль знаний и проверка применения знаний на практике.

Разработанные рекомендации и обучающий курс являются одним из средств осуществления комплексной защиты корпоративной информационной системы.

Данное утверждение подтверждается в результате экономической оценки эффективности рекомендаций по выбору средств защиты корпоративной информационной системы образовательной организации ГБПОУ «Южно-Уральский государственный технический колледж». В данную оценку вошли расчет стоимости внедрения межсетевого экранирования для защиты корпоративной информационной системы образовательной организации и сравнение со стоимостью возможного ущерба со стороны регуляторных рисков. В результате сравнения экономическая эффективность разработанных рекомендаций составила 110 230 руб.

Учитывая данный показатель, можно сделать вывод, что реализация данного проекта экономически эффективна.

Результаты исследования рекомендуется использовать в практической деятельности образовательных организаций среднего профессионального

образования с целью повышения эффективности защиты корпоративной информационной системы.

Таким образом, цель работы достигнута, задачи выполнены, гипотеза исследования подтвердилась.

СПИСОК ИСПОЛЬЗОВАННЫХ ИСТОЧНИКОВ

1. Автоматизированные системы. Защита от несанкционированного доступа к информации. Классификация автоматизированных систем и требования по защите информации [Электронный ресурс]: [руководящий документ ФСТЭК от 30.05.1992 г., с ред. от 09.12.2022 г.]. – Режим доступа: https://fstec.ru. Дата обращения: 10.05.2022.

2. Антивирусная программа // Wikipedia [Электронный ресурс]: – URL: https://ru.wikipedia.org/wiki/Антивирусная_программа/ (дата обращения: 15.05.2022).

3. Артемов А. В. Информационная безопасность : курс лекций / А. В. Артемов. – Орел : Межрегиональная Академия безопасности и выживания (МАБИВ), 2014. – 256 с.

4. Аутентификация // Wikipedia [Электронный ресурс]: – URL: https://ru.wikipedia.org/wiki/Аутентификация/ (дата обращения: 15.05.2022).

5. Ашарчук Л. М. Корпоративные информационные системы : курс лекций для студентов экономических специальностей / Л. М. Ашарчук, С. В. Карпенко, С. В. Кравченко. – Гомель: учреждение образования «Белорусский торгово-экономический университет потребительской кооперации», 2019. – 156 с.

6. Базовая модель угроз безопасности персональных данных при их обработке в информационных системах персональных данных деятельности [Электронный ресурс]: [базовая модель ФСТЭК РФ от 15.02.2008 г.]. - Режим доступа: www.consultant.ru. Дата обращения: 20.03.2023.

7. Банк данных угроз безопасности информации // bdu.fstec.ru [Электронный ресурс]. – URL: https://bdu.fstec.ru/threat-section (дата обращения: 20.03.2023).

8. Голембиовская О.М. Автоматизация мониторинга защищенности информационных систем персональных данных / О. М. Голембиовская // Сборник научно- практических статей «Развитие регионов, как фактор

укрепления единства и целостности государства». – Рыбница: 2012.– № 2. – С.63-68.

9. Голембиовская О.М. Формализация критериев выбора состава средств защиты информационных систем на основе оценки показателей угроз и уязвимостей / О. М. Голембиовская, В. И. Аверченков, М. Ю. Рытов // Информация и безопасность. – Воронеж, № 4, 2019. – С. 31-37.

10. ГОСТ Р 50922-96. Защита информации. Основные термины и определения.

11. ГОСТ Р ИСО/МЭК 14764-2002. Сопровождение программных средств.

12. Государственный реестр сертифицированных средств защиты информации // reestr.fstec.ru [Электронный ресурс]. – URL: https://reestr.fstec.ru/reg3 (дата обращения: 05.04.2023).

13. Додонов А. Г. Корпоративные информационные системы: обеспечение живучести / А. Г. Додонов, Е. В. Флейтман // Математические машины и системы. – 2005. – № 4. – С. 118–130.

14. Забуга А. А. Теоретические основы информатики. Учебное пособие. Стандарт третьего поколения / А.А. Забуга. – Санкт-Петербург : Питер, 2021. – 208 с.

15. Защита информационных систем // irsural [Электронный ресурс]. – URL: https://irsural.ru/nashi-uslugi/zashita-konfidecialnoi-informacii/zashita-informacionnyh-sistem/ (дата обращения: 15.05.2022).

16. Идентификация (информационные системы) // Wikipedia [Электронный ресурс]: – URL: https://ru.wikipedia.org/wiki/Идентификация (информационные системы)/ (дата обращения: 15.05.2022).

17. Информационная безопасность: Учебник для студентов вузов. – М.: Академический Проект; Гаудеамус, 2-е изд. – 2017. – 544 с.

18. Касперски К. Компьютерные вирусы изнутри и снаружи. – СПб.: Питер, 2017. – С. 526.

19. Косарев В. П. Компьютерные системы и сети: Учебное пособие / В.П. Косарева и Л.В. Еремина. – М.: Финансы и статистика. – 2020. – 464 с.

20. Коуров Л. В. Информационные технологии. – Мн.: «Амалфея». – 2019. – 191 с.

21. Крат Ю. Г. Основы информационной безопасности : учеб. пособие / Ю. Г. Крат, И. Г. Шрамкова. – Хабаровск : Изд-во ДВГУПС, 2018. −112 с.

22. Лебедь С. В. Межсетевое экранирование. Теория и практика защиты внешнего периметра. – МГТУ им. Н. Э. Баумана, 2017. – 306 с.

23. Межсетевой экран Usergate C100 // usergate.com [Электронный ресурс]. – URL: https://www.usergate.com/ru/products/usergate-c (дата обращения: 05.04.2023).

24. Межсетевые экраны – виды и особенности // smart-soft.ru [Электронный ресурс]. – URL: https://www.smart-soft.ru/blog/mezhsetevye-ekrany-vidy/ (дата обращения: 05.04.2023).

25. Межсетевой экран // Wikipedia [Электронный ресурс]: – URL: https://ru.wikipedia.org/wiki /Межсетевой_экран (дата обращения: 15.05.2022).

26. Методика оценки угроз безопасности информации [Электронный ресурс]: [методический документ ФСТЭК: от 05.02.2021 г.]. - Режим доступа: https://docs.cntd.ru. Дата обращения: 20.03.2023.

27. О персональных данных [Электронный ресурс]: [федеральный закон: от 27.07.2006 г. № 152-ФЗ, в ред. от 04.06.2014 г. № 152-ФЗ]. - Режим доступа: www.consultant.ru. Дата обращения: 10.05. 2022.

28. О стратегии национальной безопасности Российской Федерации [Электронный ресурс]: [указ президента РФ от 02.07.2021 № 400]. – Режим доступа: www.consultant.ru. Дата обращения: 10.05. 2022.

29. Об информации, информационных технологиях и о защите информации [Электронный ресурс]: [федеральный закон: от 27.07.2006 г. №149-ФЗ, в ред. от 06.04.2011 г. № 149-ФЗ]. – Режим доступа: www.consultant.ru. Дата обращения: 10.05. 2022.

30. Об утверждении состава содержания организационных и технических мер по обеспечению безопасности персональных данных при их обработке в информационных системах персональных данных [Электронный ресурс]: [Приказ ФСТЭК России от 18 февраля 2013 г. № 21, в ред. от 14.05.2020 г. № 68]. – Режим доступа: https://fstec.ru/. Дата обращения: 20.03.2023.

31. Об утверждении требований о защите информации, не составляющей государственную тайну, содержащейся в государственных информационных системах [Электронный ресурс]: [Приказ ФСТЭК России от 11.02.2013 г. № 17, в ред. от 29.05.2019 г.] – Режим доступа: www.consultant.ru. Дата обращения: 20.03.2023.

32. Об утверждении требований к защите персональных данных при их обработке в информационных системах персональных данных [Электронный ресурс]: [постановление правительства РФ от 01.11.2012 г. №1119**]. –** Режим доступа: www.consultant.ru. Дата обращения: 10.05. 2022.

33. Об утверждении требований о защите информации, не составляющей государственную тайну, содержащейся в государственных информационных системах [Электронный ресурс]: [приказ ФСТЭК России от 11.02.2013 №17, в ред. от 28.05.2019 №106]. – Режим доступа: www.consultant.ru. Дата обращения: 10.05. 2022.

34. Об образовании в Российской Федерации [Электронный ресурс]: [федеральный закон: от 29.12.2012 №273-ФЗ, в ред. от 17.02.2023 №26-ФЗ]. – Режим доступа: www.consultant.ru. Дата обращения: 10.05. 2022.

35. Проблемы защиты информации на предприятии // rtmtech.ru [Электронный ресурс]. – URL: https://it-cube39.ru/news/137654/ (дата обращения: 05.04.2023).

36. Программно-аппаратная защита информации // searchinform [Электронный ресурс]. – URL: https://searchinform.ru/services/outsource-ib/zaschita-informatsii/programmno-apparatnaya/ (дата обращения: 15.05.2022).

37. Программа развития ГБПОУ «Южно-Уральский государственный технический колледж» на 2019-2023 гг. от 26.02.2019 г. № 03/668.

38. Профили защиты межсетевых экранов [Электронный ресурс]: [методический документ ФСТЭК РФ: от 12.09.2016 г.]. - Режим доступа: https://fstec.ru. Дата обращения: 05.04.2023.

39. Профиль защиты межсетевых экранов типа «А» шестого класса защиты ИТ.МЭ.А6.ПЗ [Электронный ресурс]: [методический документ ФСТЭК РФ: от 12.09.2016 г.]. - Режим доступа: https://fstec.ru. Дата обращения: 05.04.2023.

40. Разработка нормативных правовых актов, определяющих угрозы безопасности персональных данных, актуальные при обработке персональных данных в информационных системах персональных данных, эксплуатируемых при осуществлении соответствующих видов деятельности [Электронный ресурс]: [методический документ ФСБ России: от 31.05.2015 г. № 149/7/2/6-432]. - Режим доступа: https://docs.cntd.ru. Дата обращения: 20.03.2023.

41. Средства вычислительной техники. Межсетевые экраны. Защита от несанкционированного доступа к информации. Показатели защищенности от несанкционированного доступа к информации [Электронный ресурс]: [руководящий документ ФСТЭК от 25.07.1997 г., с ред. от 06.02.2023 г.]. – Режим доступа: www.consultant.ru. Дата обращения: 10.05.2022.

42. Трояны удаленного доступа (RAT) – что это такое? // it-cube39.ru [Электронный ресурс]. – URL: https://it-cube39.ru/news/137654/ (дата обращения: 20.03.2023).

43. Усова Н. А. Теория информационной безопасности и методология защиты информации : Учебно-методическое пособие / Н. А. Усова, А. В. Кораблев. – Самара : Изд-во Самар. гос. экон. ун-та, 2017. – 296 с.

44. Фишинг // rt-solar.ru [Электронный ресурс]. – URL: https://rt-solar.ru/products/solar_dozor/blog/2844/ (дата обращения: 20.03.2023).

45. Федякова Н. Н. Совершенствование информационных систем управления вузом / Н. Н. Федякова // Интеграция образования. – 2018. Т 20. – №2 (83). – С. 198-208.

46. Что такое DDOS-атаки? // aws.amazon.com [Электронный ресурс]. – URL: https://aws.amazon.com/ru/shield/ddos-attack-protection/ (дата обращения: 20.03.2023).

47. Шамова Т. И. Управление образовательными системами. Учебное пособие для вузов. / Т. И. Шамова, П. И. Третьяков, Н. П. Капустин – М.: Владос. – 2002. – 320 с.

48. Шехматов С. А. Возможности информационных технологий в управлении образовательным учреждением / С. А. Шехматов // Вопросы гуманитарных наук. – 2019. № 6 (75). – 100 с.

49. Шихнабиева Т. Ш. Об одном из вариантов разработки системы повышения качества управления образованием / Т. Ш. Шихнабиева,А. В. Брежнев // Управление образование: теория и практика. – 2017. – № 3 (27). – С. 50-57.

50. Юханова И. Ю. Значение информационных технологий в управлении организацией в современных условиях / И. Ю. Юханова // Успехи современной науки и образования. – 2019. – № 1. – С. 12-13.

51. Ямалетдинова А. М. Современные информационные и коммуникационные технологии в учебном процессе / А. М. Ямалетдинова // Вестник Башкирского университета. – 2016. № 4. – С. 990-995.

52. Яценко А. И. Проект автоматизации управления административной и методической деятельностью в образовательном учреждении как условие повышения качества образовательного процесса / А. И. Яценко // Вестник Российского университета дружбы народов. Серия «Информатизация образования». – 2018. – Т. 14. № 1. С. 76-82.

53. Backdoor // itglobal [Электронный ресурс]. – URL: https://itglobal.com/ru-ru/company/glossary/backdoor/ (дата обращения: 20.03.2023).

54. Stepik // stepik.org [Электронный ресурс]. – URL: https://stepik.org/catalog (дата обращения: 05.04.2023).

ПРИЛОЖЕНИЕ А

Таблица 1 – Модель угроз ГБПОУ «Южно-Уральского государственного технического колледжа»

Наименование угрозы	Вероятность реализации угрозы (Y2)	Возможность реализации угрозы (Y)	Опасность угрозы	Актуальность угрозы	Меры по противодействию угрозе	
					Технические	Организационные
1. Угрозы от утечки по техническим каналам						
1.1 Угрозы утечки акустической информации	Маловероятна	Низкая	Низкая	Неактуальная		Инструктаж пользователей в части проведения переговоров по рабочим вопросам исключительно на территории организации и с людьми, допущенными к обсуждаемой информации
1.2 Угрозы утечки видовой информации	Маловероятна	Низкая	Низкая	Неактуальная	Жалюзи на окнах; Расположение мониторов, исключающее возможность просмотра информации третьими лицами	Инструктаж пользователей в части необходимости блокировки рабочих компьютеров в случае возможности просмотра информации людьми, не допущенными к данным сведениям
1.3 Угрозы утечки информации по	Маловероятна	Низкая	Низкая	Неактуальная		

Продолжение таблицы 1

каналам побочных электромагнитных излучения и наводок (ПЭМИН)						
2. Угрозы несанкционированного доступа к информации						
2.1 Угрозы уничтожения, хищения аппаратных средств информационной системы персональных данных (ИСПДн) носителей информации путем физического доступа к элементам ИСПДн						
2.1.1 Кража персональных электронных вычислительных машин (ПЭВМ)	Маловероятна	Низкая	Низкая	Неактуальна		Контролируемая зона для организации технической защиты конфиденциальной информации; Специализированная охрана образовательной организации
2.1.2 Кража носителей информации	Маловероятна	Низкая	Низкая	Неактуальна	Хранение носителей, исключающее несанкционированный доступ	Учет носителей; Инструктаж пользователей в части запрета выноса носителей информации с территории организации и хранения носителей в защищенных местах, исключающих возможность несанкционированного доступа

Продолжение таблицы 1

2.1.3 Кража, модификация, уничтожение информации	Маловероятна	Низкая	Низкая	Неактуальна		Контролируемая зона для организации технической защиты конфиденциальной информации с ограничением доступа посторонних лиц; Ответственность за сохранность конфиденциальной информации и ее носителей в должностных инструкциях сотрудников
2.1.4 Вывод из строя узлов ПЭВМ, каналов связи	Низкая вероятность	Средняя	Низкая	Неактуальная		Контролируемая зона для организации технической защиты конфиденциальной информации с граничением доступа посторонних лиц; Ответственность за сохранность конфиденциальной информации и ее носителей в должностных инструкциях сотрудников

Продолжение таблицы 1

2.1.5 Несанкционированный доступ к информации при техническом обслуживании узлов ПЭВМ	Маловероятна	Низкая	Низкая	Неактуальна		Ремонт допущенными сотрудниками учреждения; Технологический процесс обработки информации содержит информацию о действиях в случае выхода из строя ПЭВМ
2.1.6 Несанкционированное отключение средств защиты	Низкая вероятность	Средняя	Низкая	Неактуальная		
2.2 Угрозы хищения, несанкционированной модификации или блокирования информации за счет НСД с применением программно-аппаратных средств						
2.2.1 Действия вредоносных программ (вирусов)	Низкая вероятность	Средняя	Низкая	Неактуальна	Антивирусное программное обеспечение (ПО)	Инструктаж пользователей в части действий в случае возникновения внештатных ситуаций; Технологический процесс обработки информации регламентирует действия в случае возникновения внештатных ситуаций
2.2.2 Установка ПО не связанного с	Низкая вероятность	Средняя	Низкая	Неактуальная	Настройка средств защиты	Инструктаж пользователей в части

Продолжение таблицы 1

исполнением служебных обязанностей						запрета использования на рабочих ЭВМ ПО, не задействованного ля выполнения работ; Технологический процесс обработки информации регламентирует действия администраторов безопасности в случае обнаружения ПО не имеющегося в документации на систему
2.3 Угрозы не преднамеренных действий пользователей и нарушений безопасности функционирования ИСПДн из-за сбоев в ПО, а также от угроз неантропогенного (сбоев аппаратуры из-за ненадежности элементов, сбоев электропитания) и стихийного (ударов молний, пожаров, наводнений и т.п.) характера						
2.3.1 Утрата атрибутов доступа	Маловероятна	Низкая	Низкая	Неактуальна		Инструктаж пользователей в части организации хранения в строго определенных местах парольных карточек; Журнал учета паролей
2.3.2 Непреднамеренная модификация (уничтожение_	Низкая вероятность	Низкая	Низкая	Неактуальна	Настройка средств защиты; Резервное копирование информации	Инструктаж пользователей в части строгого исполнения порядка работ, предусмотренного для

Продолжение таблицы 1

информации сотрудниками						исполнения служебных обязанностей
2.3.3 Непреднамеренное отключение средств защиты	Маловероятна	Низкая	Низкая	Неактуальна	Доступ к установлению режимов работы средств защиты предоставляется только администратору; Настройка средств защиты	Инструктаж пользователей в части запрета каких-либо действий в отношении средств защиты
2.3.4 Выход из строя программно-аппаратных средств	Низкая вероятность	Средняя	Низкая	Неактуальна	Резервное копирование информации	
2.3.5 Сбой системы электроснабжения	Маловероятна	Низкая	Низкая	Неактуальна	Использование источников бесперебойного питания для серверов	
2.3.6 Стихийное бедствие	Маловероятна	Низкая	Низкая	Неактуальна	Пожарная сигнализация	Инструкция по действиям в случае возникновения нештатной ситуации
2.4 Угрозы преднамеренных действий внутренних нарушителей						
2.4.1 Доступ к информации, модификация, уничтожение лицами, не допущенными к ее обработке	Средняя вероятность	Средняя	Средняя	Актуальна		Инструктаж пользователей в части необходимости блокировки рабочих компьютеров в случае возможности

Продолжение таблицы 1

						просмотра информации людьми, не допущенными к данным сведениям; Парольная система доступа; Разграничение прав пользователей
2.4.2 Разглашение информации, модификация, уничтожение сотрудниками, допущенным к её обработке	Средняя вероятность	Средняя	Средняя	Актуальна		Обязательства о неразглашении; Инструктаж пользователей в части проведения переговоров по рабочим вопросам исключительно на территории организации и с людьми, допущенными к обсуждаемой информации
2.5 Угрозы несанкционированного доступа по каналам связи						
2.5.1 Угрозы выявления паролей по сети	Средняя вероятность	Средняя	Средняя	Актуальна	Антивирусное ПО	
2.5.2 Угрозы навязывания ложного маршрута сети	Средняя вероятность	Средняя	Средняя	Актуальна	Использование межсетевого экрана	

Продолжение таблицы 1

2.5.3 Угрозы внедрения ложного объекта в ИСПДн	Средняя вероятность	Средняя	Средняя	Актуальна	Использование межсетевого экрана	
2.5.5 Угрозы внедрения по сети вредоносных программ	Средняя вероятность	Средняя	Средняя	Актуальна	Антивирусное ПО; Использование межсетевого экрана	Инструктаж пользователей в части порядка действии в случае возникновения внештатных ситуаций