МИНИСТЕРСТВО ПРОСВЕЩЕНИЯ РФ
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

Реализация ролевого доступа к информации в образовательной организации

Магистерская диссертация
44.03.04 Профессиональное обучение по направлению
Управление информационной безопасностью в профессиональном образовании

Проверка на объем заимствований:
85 % авторского текста

Работа рекомендована к защите
«11» января 2024 г.
Зав. кафедрой АТИТ и МОТД
_____Руднев В.В.

Выполнил: магистрант группы
ЗФ-309-210-3-1
Юсупов Рамиль Фазылович

Научный руководитель:
К.т.н, доцент кафедры АТ, ИТ и МОТД ППИ
Руднев Валерий Валентинович

Челябинск – 2024

СОДЕРЖАНИЕ

ВВЕДЕНИЕ

Одним из наиболее значимых ресурсов образовательных организаций, является информация, в связи с чем, необходимость защиты информационных систем образовательных организаций будет первоочередной в ряду актуальных задач.

От того, насколько эффективно функционирует информационная система организации и насколько защищена циркулирующая в ней информация, во многом зависит действенность усилий педагогов при осуществлении образовательного процесса и результативность самой организации по исполнению государственной задачи подготовки высококвалифицированных специалистов.

Посредством информационной системы осуществляются: быстрый доступ ко всем необходимым данным в понятном для руководителя формате, упрощение процесса регистрации, хранения и обработки информации пользователей системы, формирование единого информационного пространства, уменьшение финансовых и трудовых затрат на организацию процессов планирования, управления и учёта деятельности организации и др.

Как правило 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.

Вопросами защиты информационной системы образовательной организации (далее – ИС ОО) 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. Шмидт и др.

Существенный вклад в развитие и решение вопросов безопасности информационных систем и информации, как ее неотъемлемого компонента,

внесли Р.М. Юсупов, В.И. Воробьёв, И.В. Котенко, А.А. Молдовян, Н.А. Молдовян, В.Ю. Осипов, И.Б. Саенко и другие.

На основе анализа научных, статистических и нормативных информационных источников можно выделить 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 ИС ОО 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, на каждом этапе обработки информации, в любой стадии жизненного цикла

ИС ОО: должна регламентно осуществляться регистрация и анализ протекающих процессов, должно быть разграничение и контроль доступа к ресурсам, должны проводиться протоколирование и аудит событий, инцидентов и т.д.

Общий анализ текущего состояния защиты корпоративных информационных систем в образовательных организациях показывает, что средства защиты не удовлетворяют требованиям практики вследствие постоянного расширения функциональности ИС ОО, нарастание зависимости от информационной инфраструктуры и угроза уничтожения, изменения, блокирования, копирования, предоставления, распространения информации.

Специфика защиты ИС ОО состоит в том, что в них содержится большой массив персональных данных, подлежащих защите. При этом обработка, хранение и передача регулируется сводом нормативных требований, отраженных в федеральных законах и других правовых актов.

Таким образом, объективно существует **противоречие:** между потребностью применения комплексных средств защиты ИС ОО и неполнотой имеющихся средств защиты в связи со специфическими информационными процедурами в таких системах.

В связи с этим тема исследования представляется актуальной: *Реализация ролевого доступа к информации в образовательной организации.*

Целью исследования является обоснование и разработка рекомендаций по реализации ролевого разграничения доступа к информации в образовательной организации.

Объект исследования: защита информации в образовательной организации.

Предмет исследования: ролевое разграничение доступа к информации в образовательной организации.

Гипотеза исследования состоит в предположении о том, что защищенность информации образовательной организации повысится при

соблюдении рекомендаций по ролевому разграничению доступа к информации, разработанных на основе модели угроз.

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

1) изучить научно-методические основы защиты информации в образовательной организации;
2) изучить нормативно-правовые требования к выбору средств защиты информации в образовательной организации;
3) изучить особенности ролевого разграничения доступа как способа защиты информации в образовательной организации;
4) проанализировать защищенность информации в образовательной организации (ГБПОУ «Южно-Уральский государственный технический колледж»);
5) разработать рекомендации по ролевому разграничению доступа к информации в образовательной организации (ГБПОУ «Южно-Уральский государственный технический колледж»);
6) оценить эффективность разработанных рекомендаций по ролевому разграничению доступа к информации в 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 информационной системе образовательной организации путем реализации ролевого разграничения доступа к информации, обеспечивающего способность системы противостоять актуальным угрозам и атакам.

Практическая значимость исследования заключается в разработке рекомендаций по реализации ролевого разграничения доступа к информации

информационной системы образовательной организации ГБПОУ СПО «ЮУрГТК», которые могут быть адаптированы для иной ОО СПО.

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

Апробация исследования была проведена посредством представления докладов на научных конференциях и печати статей:

1. VI Областная студенческая научно-практическая конференция: «ОБЕСПЕЧЕНИЕ КОМПЛЕКСНОЙ БЕЗОПАСНОСТИ ОБЩЕСТВА И ЛИЧНОСТИ: ПРОБЛЕМЫ И РЕШЕНИЯ». Публикация: «Разграничение доступа к информации в образовательной организации» / [Текст] Юсупов Р.Ф. // (г. Челябинск, 20 апреля 2023 года). – Челябинск: Издательский центр ГБПОУ «ЮУГК», Выпуск 6, 2023 года, с. 122-124
2. ……

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

ГЛАВА 1. ТЕОРЕТИЧЕСКИЕ ОСНОВЫ РЕАЛИЗАЦИИ РОЛЕВОГО ДОСТУПА К ИНФОРМАЦИИ В ОБРАЗОВАТЕЛЬНОЙ ОРГАНИЗАЦИИ

1.1. Научно-методические подходы к защите информации 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 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 «информационная система образовательной организации» (далее – ИС ОО) мы будем понимать открытую интегрированную систему реального времени, автоматизирующую управленческие процессы организации.

Основная задача и цель ИС в ОО 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.

ИС ОО 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 этих целей.

– 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, ИС ОО 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 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 ИС ОО 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 ИС ОО 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.

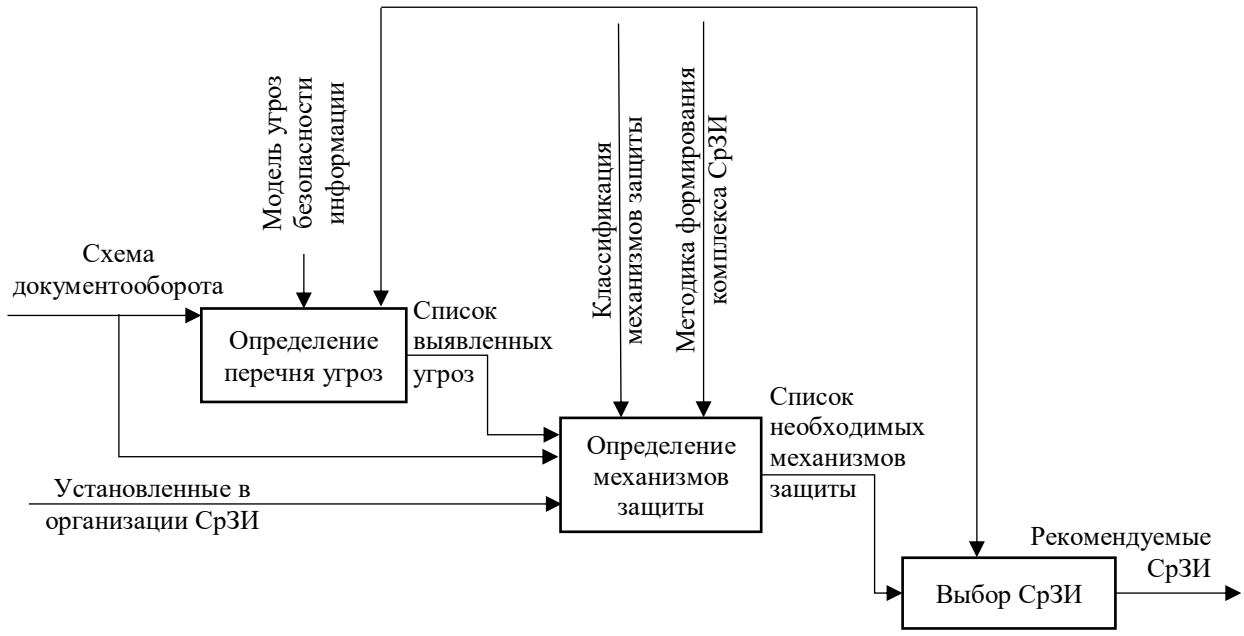
5. Сохранность данных. Позволяет сохранить данные в надежном месте и обеспечить их восстановление в случае потери.

Для защиты ИС ОО 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 – Схема рекомендуемых средств защиты информации.

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

1.2 Нормативно-правовые требования к защите информации в 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 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 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].

Такова законодательная база, отражающая совокупность требований к защите информации в образовательных организациях.

1.3. Ролевое разграничение доступа как компонент комплексной защиты информации в образовательной организации

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

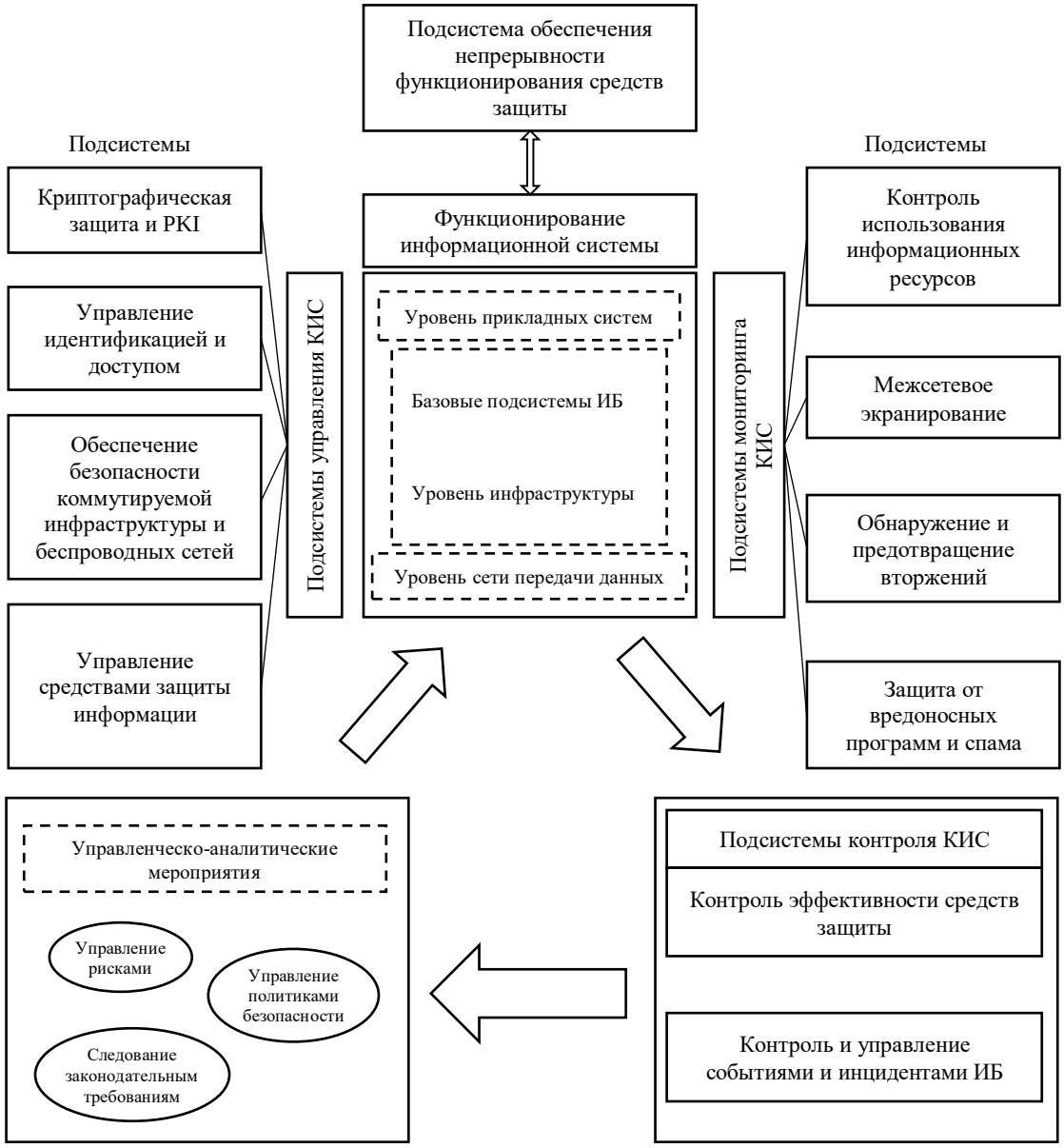


Рисунок 2 – Общая структура комплексной системы защиты информации

Поскольку каждый элемент комплексной системы безопасности важен и может играть ключевую роль, остановимся подробнее на рассмотрении такого направления обеспечения информационной безопасности как разграничение

доступа. Изначально это направление относилось к организационным мерам (таким как «управление рисками», «управление политиками безопасности», «управление идентификацией и доступом» - см. рис. 2) однако, впоследствии реализация его была осуществлена и в программно-аппаратных средствах.

При выборе средств защиты информации нужно учитывать, что существует несколько принципов защиты от несанкционированного доступа:

- 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].

В образовательных организациях 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).

В каждой образовательной организации имеется свод документов, определяющих политику информационной безопасности.

Политики контроля доступа (политики разграничения доступа) – это набор правил, определяющих и контролирующих действия каждого пользователя в системе. Политики основаны на моделях контроля доступа – математически формализованных системах, включающих в себя субъекты (пользователи/ процессы), объекты (данные/ документы/ файлы) и правила доступа, по которым вычисляется возможность выполнения субъектом. набора операций над объектом.

Среди моделей контроля доступа можно выделить три наиболее распространенных: MAC (Mandatory Access Control / Мандатный контроль доступа), DAC (Discretionary Access Control / Дискреционный контроль доступа), RBAC (Role-Based Access Control / Ролевой контроль доступа).

Дискреционная модель доступа (Discretionary access control - DAC) основана на присвоении каждой паре «субъект-объект» набора разрешенных операций доступа (READ - чтение, WRITE - запись, EXECUTE - выполнение). При запросе доступа к определенному объекту система ищет искомого субъекта в списке прав доступа данного объекта. Если субъект найден в списке и тип запрашиваемой операции включен в список разрешений, система дает разрешение на доступ, в противном случае субъекту отказывается в доступе. Дискреционная модель реализуется в виде списков контроля доступа (ACL, access control list) или матриц контроля доступа (ACM, access control matrix) (рис. 3)

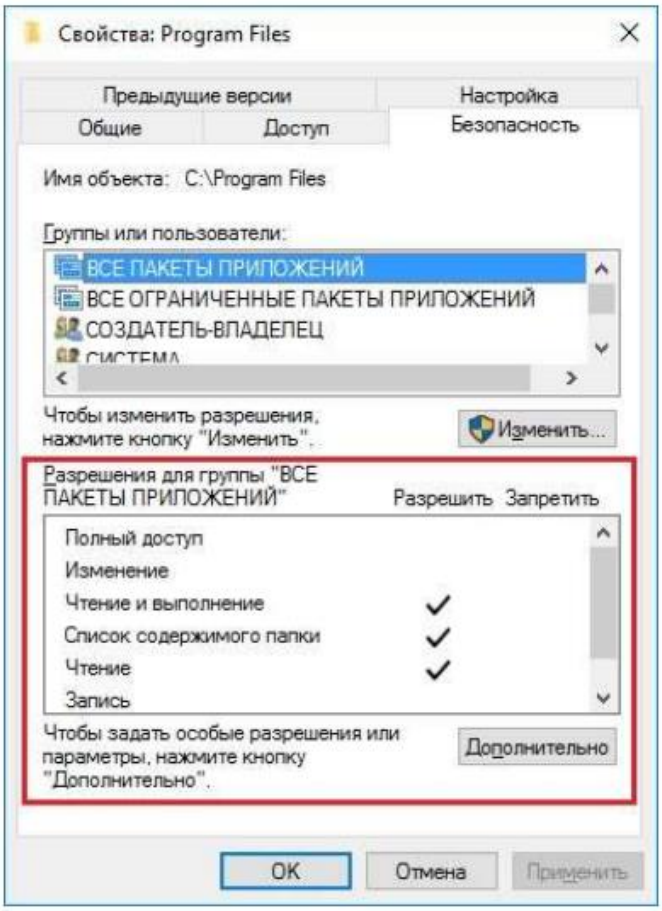


Рисунок 3 – пример реализации дискреционного доступа с помощью GUI Windows

Мандатная модель доступа (Mandatory access control - MAC) основана на классификации объектов и субъектов системы. Каждому объекту и субъекту системы присваивается определенный уровень безопасности (УБ). Уровень безопасности, обычно, описывает значимость данного объекта возможный ущерб, который может быть причинен при доступе к данному объекту. Уровень безопасности субъекта является уровнем доверия к данному субъекту.

Ролевой метод управления доступом позволяет контролировать доступ пользователей к информации, основываясь на типах их активности в системе. Данный метод подразумевает определение ролей пользователей в системе. Понятие «роль» в данном методе можно определить, как совокупность связанных с некоторым видом деятельности привилегий и обязанностей. Так,

вместо указания всех типов доступа для каждого пользователя к каждому объекту можно указать лишь тип доступа к объектам для роли, а пользователям, соответственно, указать роли. Таким образом, пользователь, «исполняющий» определенную роль, имеет доступ, соответствующий данной роли.

Ключевой особенностью ролевой модели разграничения доступа является то, что весь доступ к информационным системам и ресурсам предоставляется только через роли. Роль – это набор прав доступа. Пользователи получают доступ только через присвоенные им роли.

Идея предоставления доступа на основе ролей возникла из необходимости группировки наборов прав в какие-то отдельные сущности, которые четко давали бы понять, какой доступ есть у пользователя, с которыми было бы удобнее и понятнее работать в случае изменений как положения пользователя в организации, так и набора прав доступа пользователя. Исторически сложилось, что наборы прав стали привязывать к должностям сотрудников, по сути – к функциональным ролям.

Преимущества ролевого управления доступом состоит в следующем:

- возможность построения иерархии ролей с наследованием набора прав, что позволяет упростить ролевую модель, особенно в организациях с разнородной инфраструктурой, где используется много информационных систем, при этом с изменением штатной иерархии нет необходимости повторно указывать права в нескольких подобных ролях, достаточно поместить их в одну большую роль, как дочерние, указав лишь уникальные права для каждой роли;
- при необходимости изменения набора прав большому количеству пользователей достаточно изменить набор прав в роли;
- возможность реализации принципа разделения полномочий (SoD – Segregation of Duties), что значительно снижает риск предоставления

пользователям избыточных полномочий, например, когда две роли не могут быть в один момент времени назначены одному пользователю;

- при проектировании, внедрении и использовании ролевой модели управления доступом принимаются в расчёт факторы, которые могут привести к серьезным потерям времени и средств.

При разработке и внедрении ролевого ограничения доступа к информации необходимо учитывать следующие особенности этого метода защиты информации.

Во-первых, «разнообразие пользователей»: на практике в крупных организациях может оказаться достаточно большое количество пользователей с уникальными правами, при этом некоторые из них могут быть на одной должности, а то и в одном подразделении. Это усложняет построение ролевой модели и может привести к ситуации, когда каждому пользователю необходима своя уникальная роль. Такие ситуации могут возникнуть, когда сотрудник «вырос» в рамках своей должности или у него просто есть уникальные функции в рамках своего подразделения. Это может стать серьезной проблемой для системы управления доступом:

В таком случае трудно определить "разумно малый" набор ролей, которые отвечают за права доступа основной массы пользователей.

Непрактично создавать столько же ролей сколько пользователей – это равносильно ручному управлению доступом.

Во-вторых, «слишком много ролей»: это не всегда так, но может случиться такая ситуация, когда при подключении к системе управления доступом еще одной управляемой системы, роли, определенные для ранее подключенных систем, необходимо раздробить на несколько других ролей, с учетом всех возможных вариантов использования совместно с новой системой. Если таких новых систем несколько, то может возникнуть ситуация, когда ролей окажется больше чем пользователей.

В-третьих, «изменение обязанностей пользователей и реорганизация бизнеса»: даже если ролевая модель отражает текущую ситуацию в

организации, ее необходимо поддерживать в актуальном состоянии, отслеживать изменения обязанностей пользователей и оперативно вносить изменения в ролевую модель.

В-четвёртых, «стоимость»: необходимо учитывать, что разработка и поддержка ролевой модели в итоге может стоить дороже ручного администрирования. Кроме того, управление ролевой моделью требует более квалифицированных специалистов, чем администратор, который предоставляет права.

Однако, необходимо отметить, что использование RBAC (управление доступом на основе ролей - Role Based Access Control) уже давно считается лучшей практикой при разработке приложений, серверов баз данных и операционных систем как в нашей отечественной практике, так и в зарубежной.

Требования безопасности обычно сводятся к многофакторной идентификации и аутентификации пользователя для его авторизации в системе. Аутентификация пользователя требует ввода пароля с клавиатуры, причем систем оказывается защищенной лишь в случае пароля, состоящего из случайных символов. Такой пароль тяжело запоминается, поэтому фиксируется на бумаге, что резко повышает возможность его компрометации, и, как следствие, повышается вероятность несанкционированного доступа к системе.

Работа еще больше усложняется, если потребовать использование автоматизированного рабочего места другим пользователем, но с тем же самым кругом обязанностей, например, когда основной пользователь в командировке, отпуске и др., тем не менее современным системам ролевого доступа удается сохранить требуемый уровень безопасности без усложнения сопровождения компьютерной системы, если реализовать авторизацию пользователя по ключу на основе расписания, в котором для заданного интервала времени жестко назначать определенный компьютер для данного пользователя, выступающего в фиксированной роли.

Нужно понимать, что одно лишь использование RBAC – не панацея, необходимо параллельно продумывать и другие способы предоставления доступа – это динамические правила, запросы прав доступа, анализ атрибутов пользователей.

В больших организациях, со сложной иерархией и большим количеством разделяемых операций целесообразно использовать системы с ролевым управлением доступом (RBAC), но следует отметить, что образовательные организации не являются такими системами. Как правило, иерархия в ИС ОО достаточно проста и не превышает более четырех уровней: руководитель – администратор – преподаватель – студент.

Рассмотрим наиболее типичное представление ролевого доступа для образовательной организации СПО от предварительно построенной матрицы доступа к схеме ролевого управления доступом.

Согласно Федеральному закону от 29.12.2012 №273-ФЗ (ред. от 02.03.2016) «Об образовании в Российской Федерации», образовательные организации должны обеспечивать доступ всех желающих (родителей, учащихся, сотрудников) к уставным и локальным документам, обеспечивающим деятельность организации. В целях выполнения этого закона, лаборант размещает их на сайте и информационных стендах.

Возможность изменения и создания новых документов (файлов) есть только у директора, так как он их утверждает. Заместители в свою очередь имеют доступ лишь к чтению и записи.

Информацию о сотрудниках могут изменять и добавлять заместители директора (по управленческой структуре организации, в зависимости от линий управления), секретарь (исполняющий функции кадрового работника за неимением в образовательной организации данной ставки). Директор имеет доступ только к чтению информации, так как для изменения и добавления информации есть подчиненные.

Педагоги и кураторы имеют доступ к информации, но не в полном объеме: только то, что является кадровыми характеристиками – фамилия, имя

и отчество, стаж работы, информация о повышении квалификации, ученые степени и звания, уровень образования, должность, преподаваемые дисциплины.

Подробная информация об обучающихся необходима заместителям директора, непосредственно работающим с ними, но только для чтения и записи. Лаборанту необходим полный доступ к информации, так как именно лаборант редактирует информацию об учащихся.

Директор имеет доступ только к чтению, так как для изменения этой информации также имеются подчиненные. Для педагогов имеет важность лишь фамилия, имя, группа студента, а для кураторов нужна более подробная информация – телефон, данные о родителях и др.

Информация об успеваемости обучающихся для чтения доступна директору, заместителям директора по учебной работе, кураторам лишь в целях ознакомления себя и родителей.

Доступ к полному доступу и редактированию успеваемости обучающихся имеется только у педагогов для выставления данной успеваемости.

Предварительно составляется матрица доступа, которая может иметь вид, представленный в таблице 1.

Таблица 1- Матрица доступа образовательной организации СПО

Объект / Субъект	Документы	Подробная информация о сотрудниках	Подробная информация об обучающихся	Информация об успеваемости учащихся	Информация о повышении квалификации сотрудников
Директор	Полный доступ	Только чтение	Чтение	Просмотр	Чтение
Заместитель директора по УР	Просмотр	Полный доступ	Чтение Запись	Просмотр	Полный доступ
Лаборант учебной части	Просмотр	-	Полный доступ	Просмотр	Чтение Запись
Педагог	Просмотр	-	-	Чтение Запись	Просмотр
Куратор	Просмотр	-		Просмотр	Просмотр
Студент	Просмотр	-	-	Просмотр	Просмотр

После утверждения и согласования доступов к информационным ресурсам организации строится схема ролевого доступа – рисунок 4.

Обозначения: Полный доступ - ——, просмотр - – · –, чтение и запись - – — · –.

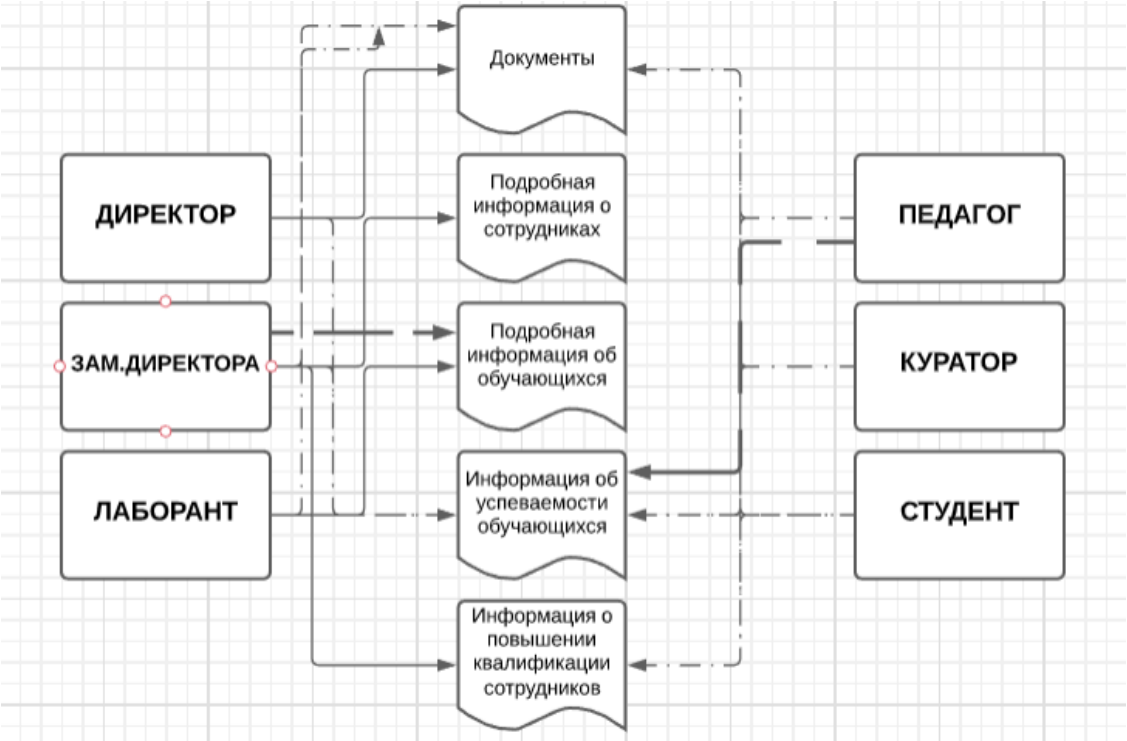


Рисунок 4. Схема ролевого управления доступом.

Таким образом, ролевая модель разграничения доступа является решением, обеспечивающим неплохие возможности в задании политики безопасности для ИС ОО, что позволяет рассматривать ролевую модель как наиболее подходящую для применения в системе управления доступом в образовательной организации, и именно поэтому ролевые модели управления доступом получили самое широкое распространение.

Вывод по первой главе

В первой главе были рассмотрены научно-методические основы защиты информации в образовательной организации. Были изучены нормативно-правовые требования к выбору средств защиты информации в образовательной организации, выявлены виды средств защиты информации.

Понятийно информационная система представляет собой взаимосвязанную совокупность средств, методов и персонала, используемых для хранения, обработки и выдачи информации в интересах достижения поставленной цели, мы понимаем информационную систему, как систему способную упорядочить и скоординировать информацию так, как это необходимо для управляющего субъекта.

При анализе научных источников было выявлено, что информационная система образовательной организации (ИС ОО) – это открытая интегрированная система реального времени, автоматизирующая управленческие процессы всех уровней и направлений деятельности, в том числе процессы принятия управленческих решений.

Информационная система в образовательной организации обеспечивает взаимодействие всех ее структурных подразделений, создавая единое образовательное пространство, в которой циркулирует значимая с точки зрения осуществления педагогического процесса информация.

Таким образом, информация неотделима от информационной системы образовательной организации и выступает одним из наиболее значимых объектов, подлежащих защите.

Информационная безопасность – это комплекс мер различного характера, направленных на реализацию защиты информации и информационной системы от несанкционированных вмешательств, хищения информации и изменения конфигурации системы со стороны третьих лиц и направленных на защиту обучающихся от любых видов пропаганды и рекламы, запрещенной законом информации.

Для защиты информации 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 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 информации, в частности, и информационной системы в целом 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.

Реализация ролевого доступа к информации в образовательной организации позволяет в составе комплексной системы защиты обеспечить надлежащий уровень защиты.

ГЛАВА 2. РАЗРАБОТКА РЕКОМЕНДАЦИЙ ПО РЕАЛИЗАЦИИ РОЛЕВОГО РАЗГРАНИЧЕНИЯ ДОСТУПА К ИНФОРМАЦИИИ ОБРАЗОВАТЕЛЬНОЙ ОРГАНИЗАЦИИ

2.1 Анализ защищенности информации в образовательной организации ГБПОУ «Южно-Уральский государственный технический колледж»

В качестве объекта защиты, базы исследования, 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: информационная система; информационные справочные системы; поисковые системы.

ИС ОО 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 управления. Наиболее развитые ИС ОО 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 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 ИС ОО.

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 5) [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.

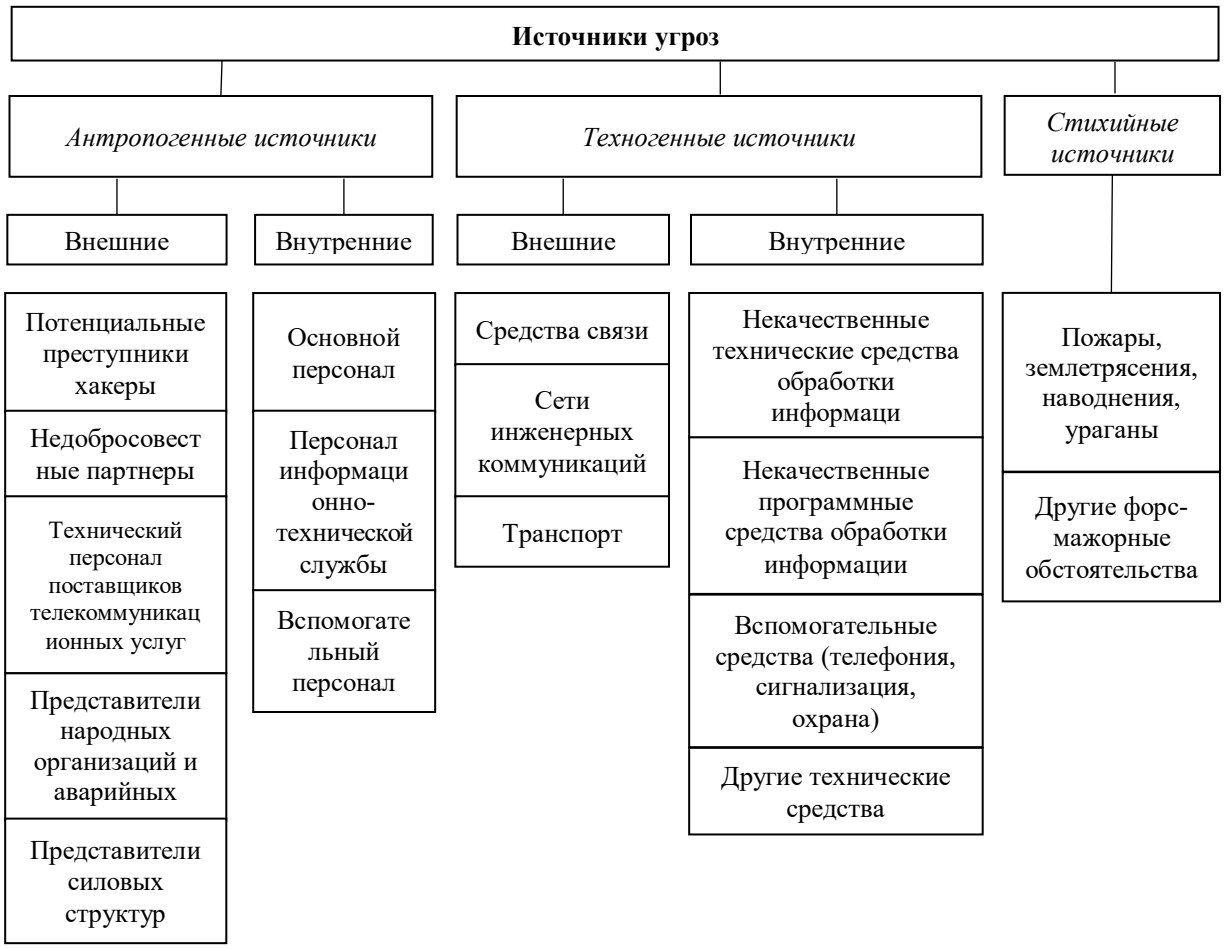


Рисунок 5 – Классификация источников угроз

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 ИС ОО.

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 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 ИС ОО:

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 отличие 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].

Для проведения анализа уязвимостей 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 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.

Далее необходимо определить частоту (вероятность) реализации угрозы (коэффициент Y2) – показатель, характеризующий, насколько вероятным является реализация конкретной угрозы безопасности информации 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 информации недостаточны;

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

При составлении перечня актуальных угроз безопасности информации в 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.

В результате была разработана модель угроз для ГБПОУ «Южно-Уральского государственного технического колледжа», представленная в

приложении А. В модели угроз отражены все возможные угрозы информационной системы образовательной организации, дана вероятностная оценка реализации угрозы и представлены возможные меры по исключению риска наступления данного события.

2.2. Разработка рекомендаций по реализации ролевого разграничения доступа к информации в 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].

Исходя из этого положения крупные компании и организации как правило применяют аппаратно-программные комплексы.

Применение программно-аппаратных комплексов характеризуется следующими преимуществами:

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

– простота в управлении, так как 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 в своих информационных массивах хранит большой объем конфиденциальной информации, для обеспечения защиты которого 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 различные комплексы, обеспечивающие разграничение доступа к информации, как программные, так и аппаратные [6].

Для сертификации программно-аппаратного комплекса (далее – ПАК) ФСТЭК определяет его профиль защиты. Профиль нужно знать, чтобы понять, в какой конкретно системе, с какими целями и для защиты каких данных можно использовать ПАК.

Меры, профили и уровни защиты информации регламентируются методическим документом «Меры защиты информации в государственных информационных системах ФСТЭК России», утв. ФСТЭК РФ 11 февраля 2014 года.

Нами был проведен мониторинг существующих ПАК для реализации разграничения доступа к информации отечественных производителей.

В результате для сравнения были выбраны следующие ПАК:

- Система разграничения доступа «КРИПТОН-ЩИТ»;
- Система контроля и разграничения доступа «Diamond ACS»;
- ПАК СЗИ НСД Аккорд-X;
- Dallas Lock 8.0-K, СЗИ Dallas Lock 8.0-K;
- Аппаратно-программный модуль доверенной загрузки «Соболь».

Выбор критериев для анализа обосновывался значимостью для ИС ОО того или иного функционала названных ПАК.

Система разграничения доступа «КРИПТОН-ЩИТ» представляет собой аппаратно-программный комплекс средств защиты информации, предназначенный для защиты от несанкционированного доступа к информации в 32 и 64-битных операционных системах Microsoft Windows. «КРИПТОН-ЩИТ» функционирует как на автономных персональных компьютерах, так и на средствах вычислительной техники, объединенных в локальную сеть.

Система «КРИПТОН-ЩИТ» соответствует всем требованиям руководящих документов Гостехкомиссии (ФСТЭК России) по уровню защиты гостайны – реализуя мандатный и ролевой принцип разграничения доступа по набору иерархических и неиерархических категорий и используя полную матрицу доступа «пользователи-процессы-ресурсы».

Система «КРИПТОН-ЩИТ» работает на уровне микроядра операционной системы, независимо от встроенных в ОС средств контроля доступа, и отличается низкими системными требованиями. «КРИПТОН-ЩИТ» не изменяет системные файлы Windows.

Основные возможности:

Идентификация и аутентификация пользователей

- Реализована единая и одноразовая идентификация и аутентификация для пользователя, с формированием профиля прав доступа;
- Контроль доступа к ресурсам компьютера;
- Контроль целостности операционной среды методом контрольного суммирования;
- Мандатный и дискреционный принцип разграничения доступа к ресурсам ОС;
- Интегрированная настройка и описание пользователей, прав доступа пользователей к ресурсам;
- Автоматическая блокировка доступа к ресурсам персонального компьютера во время отсутствия пользователя (период неактивности

пользователя, характеризующийся отсутствием работы с клавишами клавиатуры и мыши);

- Возможность трассировки обращений к ресурсам программного обеспечения в специальном отладочном режиме;
- Разграничение доступа к процедурам (программам);
- Обеспечение единого интерфейса пользователя для работы с процедурами (программами), одновременно выполняющего разграничение доступа к процедурам для каждой категории пользователя;
- Ролевая модель разграничения доступа к процедурам (программам);
- Поддержка многошаговых процедур с возможностью наследования полномочий и без него.

Интеграция с аппаратными средствами защиты

Система разграничения доступа «КРИПТОН-ЩИТ» интегрирована с изделиями семейства АПМДЗ «КРИПТОН-ЗАМОК», изделиями семейства «КРИПТОН-AncNet», шифраторами дисков семейства «КРИПТОН-ПШД», а также абонентскими шифраторами серии «КРИПТОН», что позволяет существенно повышать уровень защиты за счет дополнительных криптографических возможностей.

Разграничение и контроль доступа к периферийным устройствам

- Дополнительное разграничение доступа к USB-устройствам, регистрация данных при печати файлов на принтере;
- Гибкая система протоколирования и аудит событий в системе защиты информации;
- Поддержка двух журналов аудита пользователя – учета событий и обращений к ресурсам. Кроме того, ведется журнал печати;
- Автоматизированные средства построения профилей (белый список), контроль отладочных регистров;
- Динамический контроль целостности;

Система контроля и разграничения доступа «Diamond ACS»

Комплекс предназначен в первую очередь для обеспечения безопасности в сложных распределенных автоматизированных системах. Diamond ACS ™ используется для защиты конфиденциальной информации, персональных данных и государственной тайны.

Комплекс имеет сертификат ФСТЭК России, подтверждающий соответствие требованиям РД СВТ - по 3 классу, РД НДВ - по 2 уровню контроля, а так же возможность использования в АС до классов 1Б, 2А и 3А и ИСПДн до 1 класса включительно.

Базовая часть комплекса является программной, при необходимости она легко может быть оснащена дополнительными аппаратными компонентами.

Комплекс СЗИ НСД Diamond ACS ™ является уникальным сертифицированным решением полностью поддерживающим работу в инфраструктурах Citrix Xen Desktop, VMWare View и аналогах.

Доступны следующие варианты исполнения:

- Программно-аппаратный комплекс системы контроля и разграничения доступа на сетевой рабочей станции «Diamond ACS PCI-E Lt» (программный агент для установки на сетевой АРМ и аппаратный модуль PCI)
- Программно-аппаратный комплекс системы контроля и разграничения доступа на сетевой рабочей станции «Diamond ACS PCI» (программный агент для установки на сетевой АРМ и аппаратный модуль PCI)
- Программно-аппаратный комплекс системы контроля и разграничения доступа на сетевой рабочей станции «Diamond ACS PCI-E» (программный агент для установки на сетевой АРМ и аппаратный модуль PCI-E)
- Аппаратный модуль системы контроля доступа на рабочей станции в сети «Diamond ACS SA HW Lt» PCI/PCI-E (программно-аппаратный модуль)

Преимущества Diamond ACS ™

Управляемость: комплекс имеет средства централизованной гибкой настройки и администрирования, средства управления группами, пользователями, задания им прав доступа, а также средства работы с журналами регистрации событий, доступных администратору безопасности с рабочего места администратора через выделенный сервер безопасности. Такой подход позволяет:

- существенно упростить процессы развертывания, поддержки и администрирования комплекса
- значительно повысить оперативность реагирования на угрозы безопасности информации
- существенно экономить ресурсы, затрачиваемые на эксплуатацию и поддержку системы защиты информации

Совместимость: Diamond ACS ™ совместим с широким спектром программных и аппаратных компонентов различного назначения других производителей. Это позволяет включать в систему уже используемые клиентом средства защиты, достигая при этом максимального уровня безопасности.

Кросплатформенность: программные модули агента Diamond ACS Workstation ™ работают под управлением операционных систем следующих семейств:

- Windows (2000 SP4 Rollup, XP SP2 и выше, Vista, 7) x32 и x64 без ограничений
- Windows Server (2003, 2008, 2008R2)
- Linux (ядро 2.4.18 и выше)

Адаптивность: при разработке различных подсистем и компонент комплекса в основу были положены адаптивность, универсальность и совместимость. Это позволяет оперативно и быстро внедрять новый функционал в состав продукта, сохраняя при этом высокий уровень надежности и стойкость защитных свойств комплекса. Такой подход

позволяет легко интегрировать комплекс с различными системами и платформами.

Основные функции, реализуемые комплексом:

- централизованное управление системой защиты информации;
- доверенная загрузка операционной системы, в том числе контроль целостности ОС до ее загрузки;
- возможность работы в трех изолированных контурах различного уровня конфиденциальности;
- разграничение доступа пользователей к данным и приложениям на основе дискреционного или мандатного принципа контроля доступа;
- разграничение прав доступа пользователей к объектам баз данных, серверов приложений и сетевых служб;
- управление доступом пользователей к устройствам (дискам, принтерам, USB-устройствам, портам и т.д.);
- создание индивидуальной для каждого пользователя изолированной программной среды;
- статический и динамический контроль целостности приложений и данных;
- тотальный аудит системы, автоматическая регистрация системных событий в журнале;
- контроль вывода на печать и маркировка документов, содержащих конфиденциальную информацию;
- очистка оперативной памяти и памяти внешних накопителей;
- временная блокировка рабочего места;
- автоматизированный контроль защищенности.

Аппаратная часть системы контроля и разграничения доступа к СВТ представляет собой набор устройств, обеспечивающих поддержку функционирования ключевых защитных механизмов программного комплекса. На сегодняшний день созданы два модуля контроля доступа к СВТ - платы PCI и PCI Express.

Аппаратный модуль обеспечивает поддержку функций контроля и разграничения доступа к СВТ. Он позволяет реализовать физическое разделение информационных ресурсов (переключения контуров за счет аппаратной перекоммутации жестких дисков с интерфейсом SATA во время перезагрузки). Собственный высокопроизводительный 32-битный вычислительный модуль идеально подходит для доверенных вычислений.

Кроме того, существует возможность интеграции сертифицированных модулей криптографической защиты, таких как КриптоПро CSP и МагПро КриптоПакет.

Совместимость: Diamond ACS ™ совместим с широким спектром программных и аппаратных компонентов различного назначения других производителей, такими как:

- многофункциональное устройство сетевой защиты (межсетевой экран, VPN построитель и система обнаружения вторжений) «Дионис»;
- система антивирусной защиты Kaspersky Internet Security;
- система антивирусной защиты DrWeb;
- CryptoPro CSP;
- МагПро CSP;
- система защиты файлов и томов Crypto Pro EFS;
- система защиты файлов и томов TrueCrypt;
- идентификатор eToken Pro;
- идентификатор MS Key.

ПАК СЗИ НСД Аккорд-X (Регистрационный номер в реестре отечественного ПО: 2027)

Программно-аппаратный комплекс средств защиты информации (ПАК СЗИ) Аккорд-X предназначен для разграничения доступа пользователей к рабочим станциям под управлением ОС семейства Linux.

Функциональные возможности:

1. Защита от несанкционированного доступа к ПЭВМ (включая возможность ограничения разрешенных часов работы каждого пользователя);
2. Идентификация/ аутентификация пользователей до загрузки операционной системы с возможностью последующей передачи результатов успешной идентификации/аутентификации в ОС;
3. Аппаратный контроль целостности системных файлов;
4. Доверенная загрузка ОС;
5. Статический и динамический контроль целостности данных, их защита от несанкционированных модификаций;
6. Разграничение доступа пользователей, процессов, к массивам данных (объектам) с помощью дискреционного контроля доступа;
7. Разграничение доступа пользователей, процессов, к массивам данных (объектам) с помощью мандатного контроля доступа;
8. Разграничение доступа пользователей, к определенным процессам.
9. Контроль доступа к периферийным устройствам.
10. Создание индивидуальной для каждого пользователя изолированной рабочей программной среды;
11. Автоматическое ведение протокола регистрируемых событий;
12. Контроль печати на локальных и сетевых принтерах, протоколирование вывода данных на печать, маркировка распечатанных данных (в качестве маркера может выступать гриф секретности документа, имя пользователя, имя принтера, имя документа и другая служебная информация).

Основные отличительные особенности состоят в наличии собственной системы разграничения доступа (мандатный и дискреционный методы контроля доступа) - действия, разрешенные прикладным ПО.

В течение всего сеанса работы пользователя ведется подробный журнал событий, в котором фиксируются все действия пользователя (существует возможность настраивать уровень детальности журнала).

Программное обеспечение комплекса позволяет администратору безопасности информации описать любую, не противоречивую политику безопасности на основе наиболее полного набора атрибутов:

Дискреционные ПРД для объектов

R	разрешение на открытие объекта только для чтения
W	разрешение на открытие объекта для записи
X	разрешение на открытие объекта на выполнение
O	подмена атрибута R атрибутами RW на этапе открытия объекта (эмуляция разрешения на запись информации в открытый файл)
C	разрешение на создание объекта
D	разрешение на удаление объекта
N	разрешение на переименование объекта
L	разрешение на создание жесткой ссылки для объекта

l	разрешение на создание симлинка для объекта или контейнера

Дискреционные ПРД для контейнеров

M	создание каталогов
E	удаление каталогов
G	разрешение перехода в этот каталог
n	переименование подкаталогов
S	наследование прав на все вложенные подкаталоги
1	наследование прав на 1 уровень вложенности
0	запрет наследования прав на все вложенные подкаталоги

меток доступа, которые могут быть поименованы как уровни секретности либо другим, более удобным образом (количество меток допуска может достигать шестнадцати);

и параметров:

- перечень объектов и прав доступа к ним для конкретного субъекта;
- перечень объектов и прав доступа к ним для группы субъектов;
- перечень объектов, целостность которых должна контролироваться системой (статический и/или динамический контроль целостности), для конкретного субъекта;
- перечень объектов, целостность которых должна контролироваться системой (статический и/или динамический контроль целостности), для группы субъектов;
- перечень системных возможностей субъекта ();

- перечень системных настроек;
- уровень детальности журнала регистрации событий;
- назначение/изменение пароля для аутентификации;
- назначение/изменение идентификатора (ТМ, ПСКЗИ ШИПКА)
- временные ограничения - время по дням недели (с дискретностью 30 мин), в которое разрешено начало работ для данного субъекта;

Сильной стороной комплекса является наличие модуля контроля печати, который предоставляет возможность маркировки данных, выводимых на печать на сетевых и локальных принтерах, с протоколированием всех действий пользователя. Модуль контроля печати Аккорд-Х отрабатывает при печати документов из любого прикладного программного обеспечения, предусматривающего возможность вывода документа/файлов/данных на печать (не только OpenOffice и прочих текстовых редакторов). Контроль печати осуществляется на уровне подсистемы печати Linux, поэтому данные выводимые на печать из консоли также маркируются в соответствии с настройками подсистемы контроля печати Аккорд-Х.

В качестве маркера (штампа) может выступать, например, гриф секретности документа, имя пользователя, имя принтера, имя документа и другая служебная информация.

В качестве аппаратной базы комплекса может использоваться любой из контроллеров Аккорд в составе Аккорд-АМДЗ, также поддерживаются аппаратные идентификаторы пользователей, перечень которых постоянно расширяется.

Dallas Lock 8.0-K СЗИ Dallas Lock 8.0-K представляют собой программный комплекс средств защиты информации в ОС семейства Windows с возможностью подключения аппаратных идентификаторов.

Обеспечивает:

- защиту информации от несанкционированного доступа;
- поддержку виртуальных сред;

- дискреционный принцип разграничения доступа к информационным ресурсам и подключаемым устройствам в соответствии с матрицей доступа;
- аудит действий пользователей;
- контроль целостности файловой системы, программно-аппаратной среды и реестра;
- объединение защищенных ПЭВМ для централизованного управления механизмами безопасности;
- приведение АС, ГИС, АСУ ТП и систем обработки персональных данных в соответствие законодательству РФ по защите информации.

Имеет сертификат соответствия ФСТЭК России № 2720 от 25.09.2012. Производитель ЦЗИ «Конфидент».

Аппаратно-программный модуль доверенной загрузки «Соболь»

Электронный замок «Соболь» предназначен для решения следующих типовых задач:

- Защита компьютеров от несанкционированного доступа и обеспечение доверенной загрузки
- Создание доверенной программной среды для повышения класса защиты СКЗИ
- Основные возможности МДЗ «Соболь»:
- Идентификация и аутентификация
- Контроль целостности
- Аппаратный ДСЧ
- Регистрация попыток доступа
- Доверенная загрузка
- Сторожевой таймер

Имеет сертификаты соответствия ФСТЭК России и ФСБ в России. Производитель ООО «Код Безопасности».

1 мая 2022 года Президентом РФ был подписан указ № 250 «О дополнительных мерах по обеспечению информационной безопасности Российской Федерации», направленный на обеспечение информационной безопасности ряда ключевых организаций России. Одним из самых важных пунктов этого указа является установление перечня организаций, которым необходимо осуществить меры по оценке уровня защищенности своих информационных систем. К таким предприятиям относятся органы власти, госкорпорации, субъекты КИИ, стратегические и системообразующие организации и иные предприятия, созданные на основании Федерального закона. ИС ОО не относятся к таким ключевым структурам, однако, в названном документе дано определение оценке защищенности ИС.

Оценка защищенности — анализ реализованных мер защиты информации, который позволит определить степень соответствия требованиям основных нормативно-правовых актов, а также оценить реальный уровень защищенности организации от возможных угроз. В этом же документе определены функциональные критерии к средствам защиты информации. Полагаем возможным взять их в качестве критериев оценки вышеназванных комплексов, обеспечивающих разграничение доступа к информации в ИС ОО.

Анализ приведенных систем позволил выявить наилучший и приемлемый для ИС ОО, с нашей точки зрения программно-аппаратный комплекс, им является Dallas Lock 8.0, включающий помимо сервера безопасности, комплект сертифицированной установки, бессрочную лицензию.

Dallas Lock 8.0 обеспечивает защиту конфиденциальной информации от несанкционированного доступа как на персональных, портативных и мобильных компьютерах, так и на серверах, позволяет проводить аудит действий пользователей и контроль целостности файловой системы, программно-аппаратной среды и реестра, а также обладает собственными

механизмами управления ИБ и «песочницей», в которой можно запустить любое ПО и протестировать его в изолированной, защищенной среде.

СЗИ Dallas Lock выходит в редакции “К” и “С” а также в виде версии для Linux.

Dallas Lock 8.0-К — сертифицированная система защиты конфиденциальной информации накладного типа предназначена для автономных персональных компьютеров и компьютеров в составе локальной сети.

Dallas Lock 8.0-К представляет собой программный комплекс средств защиты информации в ОС с возможностью подключения аппаратных идентификаторов. Легко интегрируется в сложные сетевые инфраструктуры благодаря собственному набору сертифицированных решений.

Dallas Lock 8.0-С — сертифицированная система накладного типа для защиты конфиденциальной информации и информации, содержащей сведения, составляющие государственную тайну до уровня «совершенно секретно» включительно. Предназначена для автономных персональных компьютеров и компьютеров в составе локально-вычислительной сети, в том числе под управлением контроллера домена.

Полагаю, что обе версии допустимы для использования в ИС ОО ГПБОУ «ЮУрГТК», так как в них присутствует более расширенная система обнаружения вторжений, организовано дискреционное и ролевое управление доступом, они характеризуются высокой отказоустойчивости и восстановлением после сбоев, в систему входит также межсетевой экран.

Стоимость Dallas Lock 8.0-К колеблется от 7500 рублей до 22500 рублей, в зависимости от комплектации.

Резюмируя сказанное можно отметить, что информационную систему образовательной организации нужно защищать в обязательном порядке. Предлагаемое средство защиты, реализующее ролевое и дискреционное управление доступом к информации, снижает вероятность вторжения извне,

позволит установить ограничения на использование определенных программ сотрудниками, обеспечит защиту конфиденциальных данных в ИС ОО.

Преимуществом приобретения, установки и использования Dallas Lock 8.0 является и обстоятельство сертификации сотрудников организации для работы с помощью данного средства защиты информации, бессрочная консультационная поддержка и регулярные обучающие вебинары.

2.3 Оценка эффективности рекомендаций по реализации ролевого разграничения доступа к информации в информационной системе образовательной организации ГБПОУ «Южно-Уральский государственный технический колледж»

Для обоснования рекомендаций по реализации ролевого разграничения доступа к информации в информационной системе образовательной организации ГБПОУ «Южно-Уральский государственный технический колледж» был проведен анализ нормативно-правовых требований действующего законодательства и анализ угроз образовательной организации – в результате составлена модель угроз ГПБОУ СПО «ЮУрГТТК». Помимо сказанного в обоснование рекомендации мы включили и экономическую оценку эффективности рекомендаций.

Предварительно было проведено обследование информационной системы ГБПОУ «Южно-Уральский государственный технический колледж», которое осуществлялось во время прохождения технологической, научно-исследовательской и проектно-технологической практик. Для обследования ИС ОО проводился аудит документов, обследование помещений, сети, компьютерного оборудования, а также изучался внутренний регламент и правила внутреннего распорядка. В процессе обследования ИС ОО была составлена модель угроз для ГБПОУ «Южно-Уральский государственный технический колледж» в соответствии с нормативными документами:

- Приказ ФСТЭК России от 18 февраля 2013 г. № 21, в ред. от 14.05.2020 г. № 68 [26];
- руководящий документ ФСТЭК от 30.05.1992 г., с ред. от 09.12.2022 года [33];
- базовая модель ФСТЭК РФ от 15.02.2008 года [6];
- методический документ ФСТЭК: от 05.02.2021 года [22];
- постановление правительства РФ от 01.11.2012 г. №1119 [10];
- методический документ ФСБ России: от 31.05.2015 г. № 149/7/2/6-432 [1].

Часть существующих угроз может быть минимизирована благодаря ролевому разграничению доступу, существующие отечественные разработки для реализации данного сервиса ИБ были описаны в п.2.2.

Как было сказано ранее, стоимость стандартной версии СЗИ DALLAS LOCK 8.0. составляет 12500 рублей. Не исключено, что потребуются некоторые расширения, которые в рамках настоящего исследования уточнить не представляется возможность, так как Управление ИТ ГБПОУ «Южно-Уральский государственный технический колледж» не предоставило полноценный доступ к ИС ОО, что обусловлено требованиями безопасности. При оценке экономической эффективности будем исходить из минимального стоимостного показателя.

На основе проведенного анализа функциональных возможностей, а также учитывая оценку специалистов в области информационной безопасности посредством изучения их публикаций (публикационный анализ) в открытых источниках:

- https://www.anti-malware.ru/reviews/Dallas_Lock_8_0 - [Электронный ресурс] - режим доступа 14 мая 2023 года;
- https://www.youtube.com/watch?v=DnGmSpkhV1U - [Электронный ресурс] - режим доступа 11 апреля 2023 года;

- Ермолова Т.С. СИСТЕМЫ ЗАЩИТЫ ИНФОРМАЦИИ И ИХ МЕСТО В ПОЛИТИКЕ БЕЗОПАСНОСТИ // Форум молодых ученых. 2018. №4 (20). URL: https://cyberleninka.ru/article/n/sistemy-zaschity-informatsii-i-ih-mesto-v-politike-bezopasnosti-1 (дата обращения: 22.03.2023);
- https://softservis24.ru/catalog/Software/dl80k_c_uads_x_36m_dallas_lock_8_0_k_pravo_na_ispolzovanie%2A%2A_szi_nsd__skn_bessrochnaya_litsenziya_/- [Электронный ресурс] - режим доступа 10 февраля 2023 года и ряд других,

нами принято решение о рекомендации реализации ролевого доступа к информации СЗИ DALLAS LOCK 8.0.

СЗИ DALLAS LOCK 8.0. поставляется практически готовым к использованию, и его настройка может быть произведена обычным системным администратором.

На официальном сайте разработчика - https://dallaslock.ru/products/szi-dallas-lock-8-0/ (рис. 6) ООО «Конфидент» имеется возможность получить консультацию, рассчитать стоимость, пройти обучение.

Рисунок 6 – общий вид страницы сайта разработчика

Таблица 2 – 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

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

		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	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

	разрешение (такая лицензия) в соответствии с федеральным законом обязательно (обязательна)	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.

При сравнении стоимости рекомендованного средства СЗИ DALLAS LOCK 8.0 с размерами штрафов становится очевидным целесообразность его применения и экономическая эффективность применения, так как **стоимость рекомендованного средства защиты информации кратно меньше суммы возможного ущерба** со стороны регуляторных рисков.

Оценка экономически оптимальных параметров должна являться основой формирования конкретного технического облика СЗИ. Если не проводить тщательного анализа и не оптимизировать размер выделяемых на СЗИ средств, практически всегда руководитель организации и образовательная организация оказывается в экономическом проигрыше.

Необходимо учитывать, что реализация ролевого доступа к защищаемой информации является только компонентом общей системы информационной безопасности, однако, от функционирования отдельных элементов системы зависит общий результат работы системы.

Вывод по второй главе

Во второй главе были разработаны рекомендации по выбору средств защиты информации и ИС ОО, проведена оценка эффективности разработанных рекомендаций по реализации ролевого доступа к информации в 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 построения которой было выявлено, что ИС ОО имеет объективные, субъективные и случайные уязвимости. Она может быть подвержена пассивным и активным атакам, к наиболее вероятным относятся Backdoor, фишинг, переадресация маршрутов, взлом удалённого доступа, DoS-атака.

Определяя возможности комплексной защиты информации в ИС ОО, мы провели мониторинг и анализ существующих программно-аппаратных комплексов, с возможностью реализации ролевого доступа к информации.

В разработанных рекомендациях представлен обзор отечественных разработок и анализ применимости к ИС ОО базы исследования.

В результате мы остановили свой выбор на СЗИ Dallas Lock 8.0, так как он является оптимальным решением для образовательных организаций в силу своей компактности, удобства настройки и минимальной цены. Публикационный анализ технических информационных источников также подтвердил целесообразность выбора именно этого средства защиты информации.

Экономическая оценка эффективности рекомендаций по выбору средств защиты информации и ИС ОО ГБПОУ «ЮУрГТК», заключающаяся в сопоставлении затрат на рекомендованное СЗИ и возможный ущерб от рисков утечки конфиденциальной информации, подтвердила целесообразность выбора СЗИ Dallas Lock 8.0.

На внедрение разработанных рекомендаций образовательная организация потратит минимально 12500 рублей, тогда как стоимость возможного ущерба за нарушения в области информационной безопасности составят 370 000 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 информации в ИС ОО в соответствии с российским законодательством и актуальными угрозами безопасности. От успешного функционирования данных систем зависит эффективность образовательных организаций. Грамотное обеспечение защиты информации в информационной системе 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.

В процессе исследовательской работы были решены следующие задачи:

1) изучены методические основы защиты информации в ИС ОО и значение защиты информации для образовательной организации;

2) были проанализированы нормативно-правовые требования к выбору средств защиты ИС ОО, уделено внимание месту нормативных регулятивов в деятельности образовательной организации;

3) изучены различные виды разграничения доступа к информации, их месту в системе комплексной информационной безопасности, описан функционал и возможности технической реализации разграничения доступа; особое внимание уделено ролевому доступу;

4) проанализировано текущее состояние защищенности информации в образовательной организации (ГБПОУ «Южно-Уральский государственный технический колледж»), на основе правовых и нормативно-методических документов (ФСТЭК РФ) составлена матрица актуальных угроз для ГБПОУ «Южно-Уральский государственный технический колледж»;

5) разработаны рекомендации по ролевому разграничению доступа к информации в образовательной организации (ГБПОУ «Южно-Уральский государственный технический колледж»), в которых представлен обзор существующих отечественных разработок, включающих в себя функционал ролевого разграничения доступа, посредством публикационного анализа и анализа необходимого функционала для ИС ОО, а также с учетом модели угроз предложено СЗИ Dallas Lock 8.0. (разработчик ООО «Конфидент»)

6) произведена экономическая оценка эффективности предложенных рекомендаций по ролевому разграничению доступа к информации в образовательной организации, заключающаяся в сопоставлении затрат на рекомендованное СЗИ и возможный ущерб от рисков утечки конфиденциальной информации. Целесообразность применения СЗИ Dallas Lock 8.0. обоснована экономически.

Разработанные рекомендации являются одним из путей осуществления комплексной защиты корпоративной информационной системы.

Результаты исследования рекомендуется использовать в практической деятельности образовательных организаций среднего профессионального образования с целью повышения эффективности защиты ИС ОО.

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

СПИСОК ИСПОЛЬЗУЕМОЙ ЛИТЕРАТУРЫ

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 3 – 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		

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
2.1.3 Кража, модификация,	Маловероятна	Низкая	Низкая	Неактуальна		Контролируемая зона для организации

уничтожение информации						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
2.1.5 Несанкционированный доступ к информации при техническом	Маловероятна	Низкая	Низкая	Неактуальна		Ремонт допущенными сотрудниками учреждения; Технологический

обслуживании узлов ПЭВМ						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 исполнением служебных обязанностей	Низкая вероятность	Средняя	Низкая	Неактуальная	Настройка средств защиты	Инструктаж пользователей в части 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_ информации сотрудниками	Низкая вероятность	Низкая	Низкая	Неактуальна	Настройка средств защиты; Резервное копирование информации	Инструктаж пользователей в части строгого исполнения порядка работ, предусмотренного для исполнения служебных обязанностей
2.3.3 Непреднамеренное отключение средств защиты	Маловероятна	Низкая	Низкая	Неактуальна	Доступ к установлению режимов работы средств защиты предоставляется	Инструктаж пользователей в части запрета каких-либо действий в отношении средств защиты

					только администратору; Настройка 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 просмотра информации людьми, не допущенными к данным сведениям; Парольная система доступа; Разграничение прав пользователей
2.4.2 Разглашение информации,	Средняя вероятность	Средняя	Средняя	Актуальна		Обязательства о неразглашении;

модификация, уничтожение сотрудниками, допущенным к её обработке						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	
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