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

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

Выбор средств защиты корпоративной информационной системы образовательной организации

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

Проверка на объем заимствований:
75,11 % авторского текста

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

Выполнил:
Студент группы ЗФ-309-210-2-1
Динмухаметов Рустам Рафаилович

Научный руководитель:
кан.тех.н., доцент
Руднев Валерий Валентинович

Челябинск
2024

Содержание

ВВЕДЕНИЕ

Актуальность исследования. В настоящее время организация режима информационной безопасности становится критически важным стратегическим фактором развития любой организации, в том числе и образовательных учреждений. При этом, как правило, основное внимание уделяется требованиям и рекомендациям соответствующей нормативно-методической базы в области защиты информации. Вместе с тем многие ведущие отечественные компании сегодня используют некоторые дополнительные инициативы, направленные на обеспечение устойчивости и стабильности функционирования корпоративных информационных систем для поддержания непрерывности бизнеса в целом.

Сейчас все чаще в информационных источниках встречается понятие системного подхода при построении системы защиты информации (СЗИ). Понятие системности заключается не просто в создании соответствующих механизмов защиты, а представляет собой регулярный процесс, осуществляемый на всех этапах жизненного цикла информационной системы (ИС). При этом все средства, методы и мероприятия, используемые для защиты информации, объединяются в единый, целостный механизм — систему защиты. К сожалению, необходимость системного подхода к вопросам обеспечения безопасности информационных технологий пока еще не находит должного понимания у пользователей современных ИС.

Одним из наиболее значимых классов информационных систем, подлежащих защите, выступают корпоративные информационные системы (КИС). От их успешного функционирования во многом зависит эффективность многих современных организаций. Это масштабируемые системы, предназначенные для комплексной автоматизации всех видов хозяйственной деятельности любой организации, а также корпораций, требующих единого управления. Такие системы часто основаны на углубленном анализе данных, широком использовании систем

информационной поддержки принятия решений, электронном документообороте и делопроизводстве. Они обладают определенной спецификой как объектов защиты от информационных воздействий, которые постоянно совершенствуются.

Несмотря на предпринимаемые попытки защиты корпоративных информационных систем от воздействий они не имеют тенденций к снижению. Постоянное расширение функциональности информационных систем и нарастание зависимости от информационной инфраструктуры создаёт ситуацию, когда атаки на эту инфраструктуру могут приводить к последствиям, сравнимым с последствиями террористической активности.

Известны работы в области защиты корпоративных информационных систем от информационных воздействий. Среди них следует выделить исследования Г.В. Бабенко, Н.А. Гайдамакина, П.Н. Девянина, Д.П. Зегжды, П.Д. Зегжды, М. Лангехейнриха, М. Метцгер, Л. Хоффмана, М. Шмита и других ученых. Существенный вклад в развитие и решение вопросов безопасности информационных систем внесли Р.М. Юсупов, В.И. Воробьёв, И.В. Котенко, А.А. Молдовян, Н.А. Молдовян, В.Ю. Осипов, И.Б. Саенко и другие.

В целом анализ текущего состояния защиты КИС от этих угроз показывает, что возможности существующих систем и методов защиты во многом не удовлетворяют требованиям практики. Одним из существенных их недостатков выступает невысокая адаптивность к изменяющимся условиям и видам угроз.

Необходим поиск новых научно-технических решений, позволяющих повысить защищенность КИС от угроз в быстро меняющихся условиях обстановки. Принципиальной особенностью современных систем является их высокая сложность, которая выражается в гетерогенности компонентов, связей и информации. Эти особенности делают рассматриваемые системы особенно уязвимыми к воздействиям, которые отличаются повышенной эффективностью из-за использования различных программных и

аппаратных средств воздействия, типов информации, сценариев атаки. Такие воздействия могут быть направлены на ряд компонентов защищаемой информационной системы и создавать угрозу различным аспектам информационной безопасности - целостности (уничтожение, искажение), доступности (перегрузка каналов связи), конфиденциальности.

Таким образом, многообразие вариантов построения информационных систем порождает необходимость создания различных систем защиты, учитывающих индивидуальные особенности каждой из них. В то же время, большой объем имеющихся публикаций вряд ли может сформировать четкое представление о том, как же приступить к созданию системы защиты информации для конкретной информационной системы, с учетом присущих ей особенностей и условий функционирования. Возникает вопрос: можно ли сформировать такой подход к созданию систем защиты информации, который объединил бы в нечто единое целое усилия, знания и опыт различных специалистов? При этом желательно что бы указанный подход был универсальным, простым, понятным и позволял бы в одинаковой степени удовлетворить любые требования информационной безопасности. Практическая задача обеспечения информационной безопасности состоит в разработке модели представления системы (процессов) ИБ, которая на основе научно-методического аппарата, позволяла бы решать задачи создания, использования и оценки эффективности СЗИ для проектируемых и существующих уникальных ИС. Основной задачей модели является научное обеспечение процесса создания системы информационной безопасности за счет правильной оценки эффективности принимаемых решений и выбора рационального варианта технической реализации системы защиты информации.

Анализ состояния проблемы информационной безопасности в организациях профессионального образования позволил выявить *противоречие* между целесообразностью использования комплексных мер при реализации политики ИБ образовательного учреждения и

недостаточной защищенностью от потери или искажения данных корпоративной информационной системы образовательной организации.

Это определило проблему исследования, заключающуюся в необходимости выбора средств защиты корпоративной информационной системы в организации профессионального образования.

Таким образом, можно сделать вывод, что тема исследования «Выбор средств защиты корпоративной информационной системы образовательной организации» является актуальной, а полученные результаты имеют важное практическое значение.

Цель исследования: теоретико-методическое обоснование и разработка рекомендаций по выбору средств защиты корпоративной информационной системы в ГБПОУ «Южно-Уральский государственный технический колледж».

Объект исследования: защита корпоративной информационной системы образовательной организации.

Предмет исследования: средства защиты корпоративной информационной системы образовательной организации.

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

Задачи исследования:

– проанализировать процесс обеспечения информационной безопасности корпоративных информационных систем как объекта защиты в условиях информационных угроз;

– проанализировать защиту корпоративной информационной системы в ГБПОУ «Южно-Уральский государственный технический колледж»;

– разработать рекомендации по выбору средств защиты корпоративной информационной системы в ГБПОУ «Южно-Уральский государственный технический колледж»;

– произвести оценку эффективности разработанных рекомендаций и экономических затрат на их реализацию.

Для решения поставленных задач были использованы следующие *методы исследования:* изучение и анализ теоретико-методической литературы по теме исследования; документоведческий метод (анализ документации образовательной организации); анализ и сопоставление имеющихся средств для защиты данных; анализ и классификация собранных данных с последующим моделированием и проектированием системы защиты и выбора средств; метод апробации результатов.

Теоретической и методологической базой исследования явились нормативно-правовые акты законодательства Российской Федерации, а также труды следующих авторов: Авдеев М.Ю., Алексеев С.С., Амелин Р.В., Богатырева Н.В., Волков Ю.В., Марченко Ю.А., Федосин А.С., Бадьина А., Бархатова Е.Ю., Беспалов Ю.Ф., Сенаторова Н.В., Терещенко Л.К. Хужокова И.М., Якушев В.С.

Состояние изученности проблемы.

Общетеоретические аспекты исследования информационной безопасности представлены в публикациях Е. Б. Белова, Е. А. Ерофеева, В.Н. Лопатина, А. А. Стрельцова, В. А. Тихонова, В. В. Райх, Ю. С. Уфимцева.

Крупный вклад в развитие теории и практики информационной безопасности внесли И.И. Быстров, В.А. Герасименко, О.Ю. Гаценко, А.А. Грушо, В.С. Заборовский, П.Д. Зегжда, Д.П. Зегжда, В.А. Конявский, А.А. Малюк, А.А. Молдовян и др.

Ряд работ посвящен системно-управленческому аспекту информационной безопасности: А. А. Кононова, А. В. Манойло, С. А. Мелина, Ю. А. Родичева, Д. И. Правикова, А. С. Устинова, Д. Б. Фролова.

Процессы функционирования самих КИС исследовали А.А. Карпов, А.Л. Ронжин, А.В. Смирнов, Б.В. Соколов, А.Л. Тулупьев.

Практическая значимость работы заключается в анализе имеющихся на рынке средств защиты корпоративных информационных систем и выборе наиболее подходящих средств для внедрения в систему информационной безопасности ГБПОУ «Южно-Уральский государственный технический колледж»; возможности применения разработанных рекомендаций в других учебных заведениях СПО.

Апробация результатов исследования и их внедрение. Результаты докладывались и обсуждались:

− на Международной научно-практической конференции «Актуальные задачи теории, методологии и практики научной деятельности», 2022 г.,

− на Международной научно-практической конференции «Наука. Образование. Инновации: современное состояние актуальных проблем», 2024 г.

База исследования: ГБПОУ «Южно-Уральский государственный технический колледж».

Структура магистерской диссертации: работа состоит из введения, двух глав, заключения, списка использованных источников.

ГЛАВА 1 ТЕОРЕТИЧЕСКИЕ ОСНОВЫ ИССЛЕДОВАНИЯ ЗАЩИТЫ КОРПОРАТИВНЫХ ИНФОРМАЦИОННЫХ СИСТЕМ В ОБРАЗОВАТЕЛЬНЫХ ОРГАНИЗАЦИЯХ

1.1 Понятие корпоративной информационной системы и значение её защиты в образовательной организации

Информатизация различных сфер общественной жизни давно уже превратилась в обычное явление. Изменения, происходящие в обществе в процессе информатизации, существенно влияют и на систему образования. Так, информация и знания становятся стратегическими ресурсами государства в процессе реализации национального проекта «Образование», а доступ к ним – одним из основных факторов социально-экономического развития. Сбор, обработка, использование и передача информации являются неотъемлемым элементом успешной деятельности любого субъекта рынка. В полной мере это относится и к образовательным организациям, где накоплены значительные, но недостаточно используемые информационные ресурсы.

Отличительной особенностью современной системы образования является резкое возрастание прямых и обратных потоков информации по всей вертикали управления, поэтому современное управление образованием превращается в управление информационными потоками. Традиционные формы работы с информацией практически пережили себя, поэтому альтернативы использованию компьютерных технологий управленческого назначения нет. Хранение, обработка, получение, передача, анализ информации, уменьшение бумажного потока посредством компьютерных сетей предоставляет возможность ускорения процесса управленческой деятельности и, в целом, повышения ее эффективности [9].

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]).

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

В Федеральных государственных образовательных стандартах [3,8] предъявляются требования, реализация которых возможна только при построении единого информационного пространства образовательной организации – цифровой образовательной среды, в которой будет протекать образовательный процесс. Вопросы проектирования информационных сред и организации управления ими стали повседневными вопросами менеджмента в образовании.

В самом общем виде единое информационное пространство представляет собой систему, в которой задействованы и на информационном уровне связаны между собой все участники образовательного процесса. Иными словами, основой построения единого информационного пространства образовательной организации выступает информационная система [5]. Информационная система предназначена для того, чтобы обеспечивать информационно-коммуникационную поддержку основной и вспомогательной деятельности в образовательном процессе.

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.

В последнее время стала достаточно популярной идея построения корпоративных информационных систем. Корпоративная информационная система (КИС) – это управленческая идеология, объединяющая бизнес-стратегию предприятия (с выстроенной для ее реализации структурой) и передовые информационные технологии. «Корпоративность» в терминах КИС означает соответствие системы нуждам крупной фирмы (организации), имеющей сложную территориальную структуру [4]. Несмотря на то, что понятие корпоративности подразумевает наличие довольно крупной, территориально-распределенной информационной системы, анализ литературы показал, что к корпоративным информационным системам можно отнести системы любых предприятий (организаций), вне зависимости от их масштаба и формы собственности.

Основная цель разработки модели корпоративной информационной системы конкретной образовательной организации – создание единого информационного пространства образования. При выборе подхода к построению КИС решается вопрос о возможности использования существующих на рынке тиражируемых систем или необходимости создавать уникальную систему, полностью ориентированную только на задачи конкретной образовательной организации.

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

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

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

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

4. 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.

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

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

Для корпоративных информационных систем (КИС) характерны следующие признаки:

− «сплошная» автоматизация бизнес-процессов;

− создание единого информационного пространства для подготовки и принятия управленческих решений;

− применение средств коммуникаций и компьютерных сетей;

− организация распределенной обработки данных на различных аппаратных и программных платформах.

Важнейшим стратегическим ресурсом информационных систем является информация. Особенно это очевидно для многофункциональных,

крупномасштабных предприятий. Качество управления во многом зависит от качества информации, которое определяется полнотой, достоверностью, актуальностью и своевременностью представления информации, а также зависит от обеспечения безопасности и надежного хранения этого ресурса.

Информационные системы должны удовлетворять двум непреложным требованиям: разрабатываться достаточно быстро и быть легко адаптируемыми к постоянно меняющимся требованиям внешней среды.

Информационные системы — базы данных, электронный документооборот, системы документов, обеспечивающие подготовку принятия управленческих решений, являются весьма уязвимыми в условиях усиления конкурентной борьбы и совершенствования информационных технологий доступа к информации, расширения сферы сетевых коммуникаций. Проблема надежной и эффективной защиты информационных систем управления от угроз, нацеленных на ухудшение качества информации, физическое разрушение, несанкционированное использование или хищение информационных ресурсов, является актуальной. Решение этой проблемы потребовало разработки теории информационной безопасности и инструментальных методов исследования и реализации системы защиты информации.

Информационные системы управления должны достаточно быстро разрабатываться и легко адаптироваться к постоянно меняющимся требованиям со стороны системы и объекта управления. Потребность в защите информации от несанкционированного, случайного или злоумышленного использования, модификации или уничтожения является перманентной. Эта потребность особенно остро проявилась в последнее десятилетие в связи с расширением компьютерных сетей, обеспечивающих интеграцию большого числа пользователей, ростом масштабов систем управления предприятий.

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

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

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

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

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

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

Под информационной безопасностью мы будем понимать защищенность информации и поддерживающей инфраструктуры от случайных или преднамеренных воздействий естественного или искусственного характера, которые могут нанести неприемлемый ущерб субъектам информационных отношений, в том числе владельцам и пользователям информации и поддерживающей инфраструктуры.

Информационные системы создаются (приобретаются) для получения определенных информационных услуг. Если по тем или иным причинам

предоставить эти услуги пользователям становится невозможно, это, очевидно, наносит ущерб всем субъектам информационных отношений. Поэтому, не противопоставляя доступность остальным аспектам, мы выделяем ее как важнейший элемент информационной безопасности.

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

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

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

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

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

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

Таким образом, практической реализацией единого информационного пространства образовательной организации является создание единой корпоративной информационной системы, разработка и внедрение которой является необходимым и обязательным условием эффективного функционирования образовательной организации в современных условиях.

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

1.2 Концепция информационной безопасности корпоративной информационной системы

Информационная безопасность является одной из лидирующих качественных характеристик информационной системы. Концептуальный подход к информационной безопасности предполагает [23,26-28]:

− согласование требований экономической безопасности к информационной безопасности, к определенным информационным ресурсам;

− конкретизация вида защищенности каждого информационного ресурса и информационно-технологического компонента КИС;

− разработку единой политики безопасности КИС — совокупности правил и стандартов, регламентирующих функционирование защищенной КИС в виде «профилей защиты» ее компонентов;

− создание информационно-технологического комплекса в виде системы защиты информации (СЗИ), включающего алгоритмические, технические и программные методы и средства защиты информационно-технологических компонентов и информационных ресурсов КИС.

Информационная безопасность – многогранная, можно даже сказать, многомерная область деятельности, в которой успех может принести только систематический, комплексный подход.

Под защитой информации КИС в более широком смысле понимается комплекс организационных, правовых и технических мероприятий по предотвращению угроз информационной безопасности и устранению их негативных последствий путем создания системы защиты информационных ресурсов КИС - СЗИ. Степень защищенности информационных ресурсов должна быть необходимой и достаточной для поддержания требуемого уровня ЭБ деятельности предприятия.

Защита информации в корпоративных системах требуется:

– для организаций со сложной административно-территориальной структурой: банков, торговых сетей, государственных и транснациональных компаний, производственных комплексов;

– а также предприятий любого уровня, использующих облачные технологии, онлайн кассы, IP-телефонию, интернет-банки, системы электронного документооборота (ЭДО).

Цели и методы защиты информации определяют специфику разработки СЗИ, которая заключается в следующем.

Во-первых, СЗИ − совокупность методов и средств, направленных на обеспечение информационной безопасности, включая обеспечение конфиденциальности и целостности информации, поддержку санкционированного доступа.

Конфиденциальность информации означает соблюдение секретности, скрытность смыслового содержания для несанкционированных пользователей.

Целостность информации соответствует понятию «полнота данных» как по составу, так и по значениям данных; непротиворечивость и актуальность данных, достоверность предоставления информации.

Санкционированный доступ означает поддержку доступа для тех лиц, которые имеют на это соответствующие полномочия.

Во-вторых, защита информации является синонимом термина «обеспечение безопасности информации» или «информационной безопасности». Поскольку информационные технологии обработки охватывают все этапы обработки данных (от момента регистрации информации в документе и до выдачи пользователям), защиту информации КИС следует рассматривать для всей информационно-технологической системы обработки данных. Структурными компонентами информационно-технологической системы являются:

− технологические процессы (операции) обработки данных,

− программные средства, реализующие алгоритмы защиты данных;

− технические средства обработки,

− собственно информация (документы, база данных, хранилище данных).

Все эти компоненты находятся под влиянием деструктивных воздействий угроз (рис.1) и снижают качественные характеристики данных.

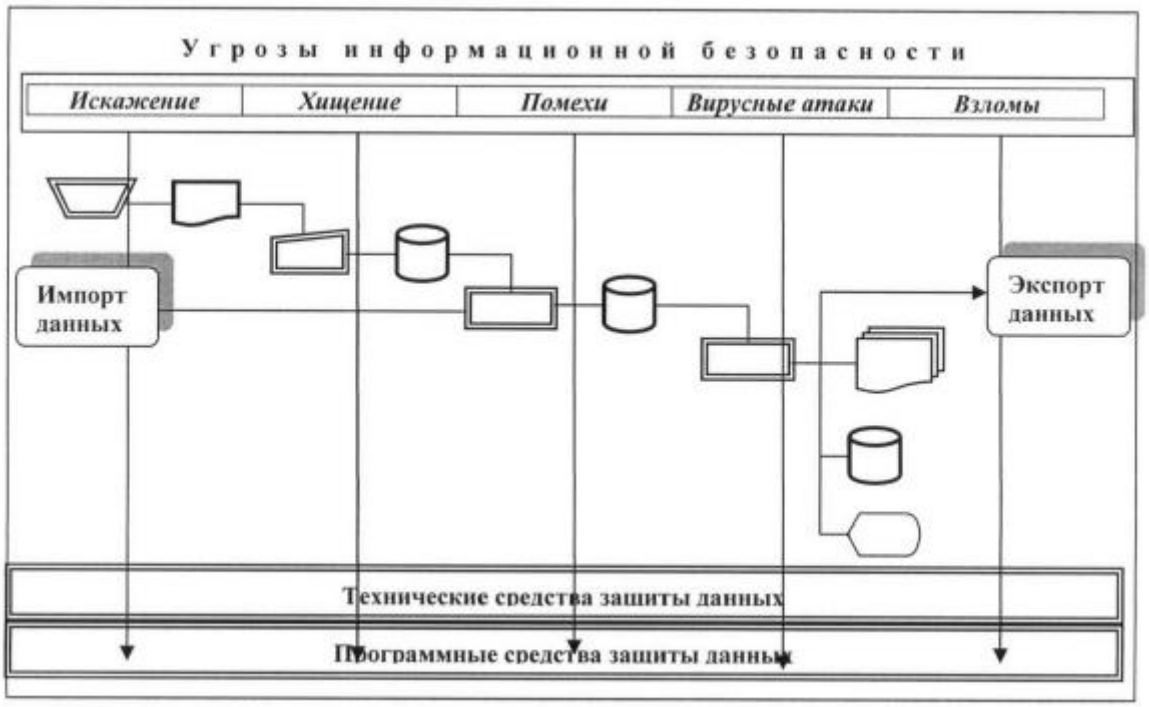

Рисунок 1 − Деструктивное воздействие угроз

В-третьих, основными функциями СЗИ, разрабатываемой как целевой подсистемы КИС, являются:

− упреждение действия угроз;

− обнаружение результатов действия угроз;

− локализацию действий угроз;

− ликвидацию негативных последствий угроз.

Упреждение угроз обеспечивается различными средствами, начиная от сознательного отношения сотрудников к проблеме информационной безопасности до создания СЗИ, сбора и анализа информации о готовящихся противоправных актах, планируемых хищениях, подготовительных действиях и других преступных деяниях.

Обнаружение угроз — это действия по идентификации видов угроз и их источников, а также видов ущерба. К таким действиям можно отнести обнаружение фактов хищения или мошенничества, разглашения конфиденциальной информации или несанкционированного доступа к источникам коммерческих секретов.

Локализация угроз направлена на определение сферы действия угрозы и конкретных ее проявлений.

Ликвидация последствий действия угрозы имеет целью восстановление состояния объектов защиты, подвергшихся разрушению, на момент наступления угрозы.

В-четвертых, СЗИ должна гарантировать правовую защиту информационных ресурсов, в том числе от противоправных посягательств, таких как:

- разглашение конфиденциальной информации;
- несанкционированный доступ к информации;
- нарушение целостности, полноты информации;
- нарушение прав владельцев (создателей) информационных ресурсов.

В-пятых, разработка концепции СЗИ КИС должна учитывать, что:

- любой информационный ресурс должен имеет «владельца» (юридические или физические лица), имеющего права на владение, распоряжение и использование информации;
- именно владелец определяет приемлемый уровень ЭБ информационного ресурса и только он может оценить экономический ущерб КИС вследствие нарушения защиты информации;
- защита информации связана с дополнительными затратами на обработку данных, что отрицательно сказывается на экономической эффективности КИС; с другой стороны, эффект от предотвращения угроз средствами СЗИ оценивается как сумма предотвращенного ущерба, и это повышает экономическую эффективность КИС, то есть любая СЗИ должна быть экономически эффективной.

Суммируя вышесказанное можно утверждать, что защита информации − комплекс мероприятий, проводимых собственником информации по защите своих прав на владение и распоряжение информацией, созданию условий, ограничивающих ее распространение и исключающих или существенно затрудняющих несанкционированный, незаконный доступ к конфиденциальной информации. Информационная безопасность КИС является обязательным условием устойчивого функционирования объекта, а также является условием реализации ЭБ деятельности предприятия.

Для достижения целей защиты информации необходимо решить ряд задач:

− выявить причины и условия, способствующие возникновению и реализации угроз, нацеленных на информационно-технологические компоненты КИС и информационные ресурсы;

− иметь прогноз вероятности появления (атак) угроз определенного вида в определенном интервале времени;

− разработать основы построения СЗИ, модели и методы построения архитектуры и выбора компонентов.

Разработку СЗИ следует выполнять на основе системного подхода, который требует комплексного изучения проблемы экономической и информационной безопасности КИС, СЗИ рассматривается как совокупность взаимосвязанных организационных, программных, технических, информационных и алгоритмических методов и средств защиты информационных ресурсов КИС, Жизненный цикл СЗИ включает этапы:

− анализ и моделирование информационной безопасности КИС;

− проектирование СЗИ;

− функционирование СЗИ (реализация защиты информационных ресурсов КИС)

− модернизация СЗИ.

На рисунке 2 представлена структура этапа анализа и моделирования информационной безопасности КИС, который в наибольшей степени определяет специфику и эффективность создаваемой СЗИ.

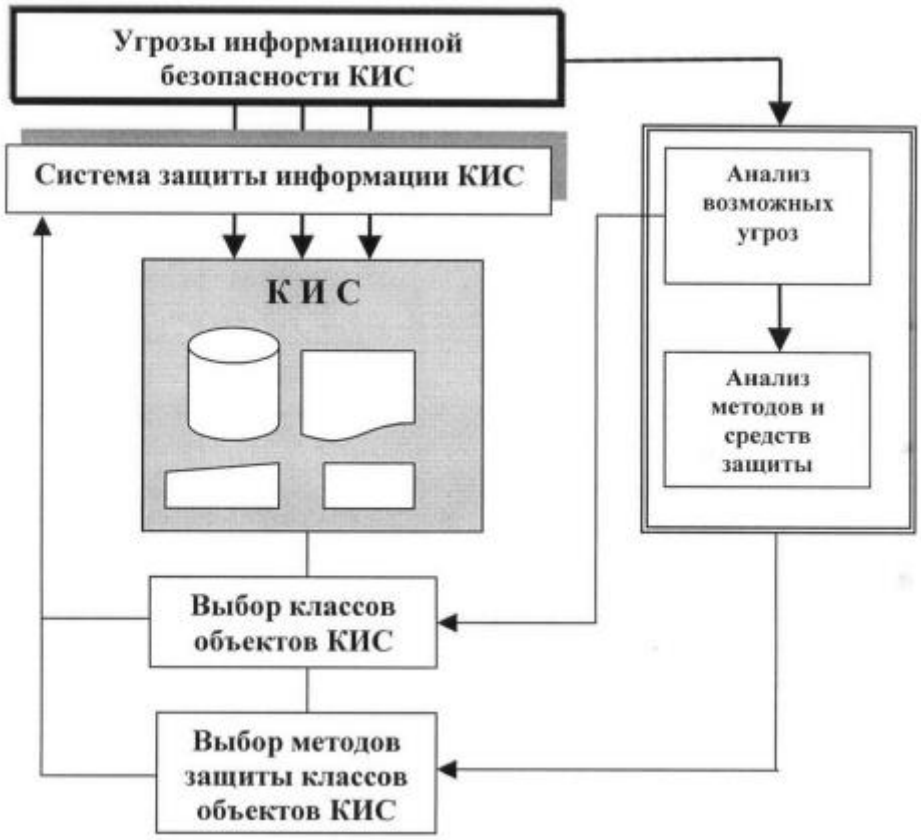

Рисунок 2 − Структура анализа и моделирования информационной безопасности

На этапе анализа и моделирования информационной безопасности КИС необходимо:

− выделить так называемые «объекты защиты» - конкретные виды информационных ресурсов и информационно-технологических компонентов КИС;

− определить свойства объектов защиты и требования со стороны обеспечения ЭБ деятельности предприятия;

− установить полный перечень угроз для информационных ресурсов и выполнить их классификации;

− определить условия и закономерность возникновения угроз (плотность вероятности, закон распределения вероятности появления угроз);

− дать оценку негативных последствий для объектов защиты (деструктивных изменений) вследствие воздействия на них угроз;

− определить методы и средства, обеспечивающие противодействие и устранение негативных воздействий угроз на объекты защиты;

− разработать модели выбора средств и методов защиты информации, оценки эффективности СЗИ КИС.

Защита информации должна осуществляться на всех технологических этапах обработки данных, относится к различным объектам защиты. Выбор средств защиты информационных ресурсов должен учитывать и технические, и экономические параметры, некоторые из них выступают в качестве ограничения; другие параметры - в качестве критериев модели синтеза оптимальной СЗИ. Ряд параметров модели будет иметь случайный характер, поэтому необходимо создание имитационной модели синтеза СЗИ КИС.

Разработка и внедрение СЗИ сказывается на модернизации подсистем КИС.

1. Правовое обеспечение - необходима разработка нормативных актов, устанавливающих правовой статус субъектов правоотношений («владельцев», «пользователей»), а также предприятия с «внешней средой» по отношению к информационным ресурсам КИС, нормативно-правовая регламентация методов и средств защиты (в том числе патентная чистота, наличие лицензий).

На основе нормативных актов следует разработать организационно-распорядительные документы действий «субъектов» (пользователей) в защищенной КИС - в виде должностных инструкций. Следует также контролировать их исполнение силами подразделения экономической и информационной безопасности предприятия.

2. Организационно-экономическое обеспечение КИС – разработка стандартов экономической безопасности, на основе которых регламентируются требования к объектам защиты КИС.

3. Техническое обеспечение — определение состава оборудования для аппаратных методов защиты информационных ресурсов и обеспечения надежной работы вычислительных систем.

4. Информационное обеспечение - проектирование и использование:

− унифицированных форм документов и структуры БД;

− единой системы классификации и кодирования технико-экономической информации;

− стандартных маршрутов движения информационных потоков КИС (схем документооборота);

− создания профилей информационной безопасности объектов защиты КИС;

− администрирования СЗИ КИС.

5.Страховое (ресурсное) обеспечение - создание оптимального уровня запасов корпоративных ресурсов для защиты от ущерба, связанного с возникновением различных угроз.

1.3 Системы защиты корпоративных информационных систем

Система защиты информации — совокупность механизмов, процедур и других управляющих воздействий, реализованных для сокращения риска, связанного с угрозой. Некоторые службы обеспечивают защиту от угроз, в то время как другие службы обеспечивают обнаружение реализации угрозы:

− идентификация и установление подлинности, является службой безопасности, которая помогает гарантировать, что в КИС работают только авторизованные лица;

− управление доступом, является службой безопасности, которая помогает гарантировать, что ресурсы КИС используются разрешенным способом;

− конфиденциальность данных и сообщений, является службой безопасности, которая помогает гарантировать, что данные КИС, программное обеспечение и сообщения не раскрыты неавторизованным

лицам;

− целостность данных и сообщений, является службой безопасности, которая помогает гарантировать, что данные КИС, программное обеспечение и сообщения не изменены неправомочными лицами;

− контроль участников взаимодействия, является службой безопасности, посредством которой гарантируется, что объекты, участвующие во взаимодействии, не смогут отказаться от участия в нем. В частности, отправитель не сможет отрицать посылку сообщения или получатель не сможет отрицать получение сообщения;

− регистрация и наблюдение, является службой безопасности, с помощью которой может быть прослежено использование всех ресурсов КИС.

Рассмотрим отдельные службы обнаружения реализации угроз.

Идентификация и аутентификация пользователей. Первый шаг к обеспечению безопасности ресурсов КИС — идентификация пользователей (проверка личности). Подтверждение проверки личности пользователя и установление подлинности пользователя называется аутентификацией. Аутентификация обеспечивает основу для эффективного функционирования других мер и средств защиты, используемых в КИС.

Оба эти средства защиты эффективны только при условии, что пользователь, использующий данную службу, действительный пользователь, которому назначен данный идентификатор пользователя. Идентификация требует, чтобы пользователь был так или иначе известен системе. Она обычно основана на назначении пользователю идентификатора. Однако КИС не может доверять заявленному идентификатору без подтверждения его подлинности. Установление подлинности возможно при наличии у пользователя уникального свойства (что он имеет или знает, делает). Чем больше количество таких свойств пользователей, тем меньше риск, что кто-то подменит законного пользователя.

Требование, определяющее необходимость аутентификации, должно существовать в большинстве политик безопасности КИС. Это требование

может содержаться неявно в политике концептуального уровня, которая подчеркивает необходимость эффективного управления доступом к информации и ресурсам КИС. В большинстве КИС используется механизм идентификации и аутентификации на основе схемы:

- идентификатор пользователя;
- пароль пользователя.

Если после рассмотрения всех вариантов аутентификации, политика КИС определяет, что системы аутентификации только на основе паролей приемлемы, то самой важной мерой защиты становится надлежащее управление созданием паролей, их хранением, слежением за истечением срока их использования, и удалением. Из-за уязвимых мест, которые все еще существуют при использовании механизмов на основе только паролей, могут использоваться более надежные механизмы. Необходимо отметить новые разработки в области систем аутентификации, основанные на смарт-картах и использовании биометрии.

Механизм, основанный на интеллектуальных картах, требует, чтобы пользователь владел смарт-картой и, дополнительно, может потребовать, чтобы пользователь знал персональный код идентификации (ПКИ-PIN) или пароль. Смарт-карта реализует аутентификацию с помощью схемы запрос/ответ, использующей указанные выше параметры в реальном масштабе времени. Использование параметров в реальном масштабе времени помогает предотвратить получение злоумышленником неавторизованного доступа путем воспроизведения сеанса регистрации пользователя. Эти устройства могут также шифровать сеанс аутентификации, предотвращая компрометацию информации аутентификации с помощью наблюдения и перехвата.

Механизмы блокировки для элементов КИС и автоматизированных рабочих мест или ПК, которые требуются для разблокировки аутентификации пользователя, могут быть полезны для тех пользователей, кто должен часто оставлять рабочее место. Эти механизмы блокировки позволяют

пользователям остаться зарегистрированными в КИС и покидать свои рабочие места (в течение определенного периода времени, не длиннее заданного), не делая при этом свое рабочее место потенциально доступным злоумышленникам.

Модемы могут потребовать дополнительной защиты. Злоумышленник, который может получить доступ к модему, может получить доступ в КИС, угадав пароль пользователя. Доступность модема для использования его законными пользователями может также стать проблемой, если злоумышленник имеет постоянный доступ к модему.

Механизмы, которые обеспечивают пользователя информацией об использовании его регистрационного имени, могут предупредить пользователя, что его имя использовалось необычным образом. Эти механизмы включают уведомления о дате, времени, и местоположении последнего успешного сеанса и числе предыдущих ошибок при регистрации.

Типы механизмов защиты, которые могли бы быть реализованы, чтобы обеспечить службы идентификации и аутентификации:

- механизм, основанный на паролях;
- механизм, основанный на интеллектуальных картах;
- механизм, основанный на биометрии;
- генератор паролей;
- блокировка с помощью пароля;
- блокировка клавиатуры,
- блокировка ПК или автоматизированного рабочего места;
- завершение соединения после нескольких ошибок при регистрации;
- уведомление пользователя о «последней успешной регистрации» и «числе ошибок при регистрации»;
- механизм аутентификации пользователя в реальном масштабе времени;
- криптография с уникальными ключами для каждого пользователя.

Управление доступом к информационным ресурсам. Эта служба защищает против неавторизованного использования ресурсов КИС. Она реализуется при помощи механизмов управления доступом и механизмов привилегий.

Большая часть файловых серверов и многопользовательских автоматизированных рабочих мест в некоторой степени обеспечивают эту службу. При монтировании томов файловых серверов ПК не осуществляют управление доступом, хотя файлы на смонтированных дисков находятся под управлением доступом ПК. Важно использовать службы управления доступом, конфиденциальности и целостности в максимально возможном объеме для ПК.

Управление доступом может быть достигнуто при использовании дискреционного управления доступом или мандатного управления доступом.

Дискреционное управление доступом — наиболее общий тип управления доступом, используемого в КИС. Основной принцип этого вида защиты состоит в том, что индивидуальный пользователь или программа, работающая от имени пользователя, имеет возможность явно определить типы доступа, которые могут осуществить другие пользователи (или программы, выполняющиеся от их имени) к информации, находящейся в ведении данного пользователя. Дискреционное управление доступом реализует решения по управлению доступом, принятые пользователем.

Мандатное управление доступом реализуется на основе результатов сравнения уровня допуска пользователя и степени конфиденциальности информации. Существуют механизмы управления доступом, которые поддерживают степень детализации управления доступом на уровне следующих категорий:

- владелец информации;
- заданная группа пользователей.

В общем случае, существуют следующие права доступа:

- доступ по чтению;

− доступ по записи;

− доступ для выполнения.

Некоторые операционные системы обеспечивают дополнительные права доступа, могут поддерживать профили пользователя и списки возможностей или списки управления доступом для большого количества отдельных пользователей и групп пользователей. Использование этих механизмов позволяет обеспечить большую гибкость в предоставлении различных прав доступа пользователей, которые могут обеспечить более строгий контроль доступа к файлам (или каталогам).

Управление доступом пользователя может осуществляться на уровне каталогов или файлов. Управление доступом на уровне каталога приводит к тому, что права доступа для всех файлов в каталоге становятся одинаковыми. Например, пользователь, который имеет доступ по чтению к каталогу, может читать (и, возможно, копировать) любой файл в этом каталоге. Права доступа к директории могут также обеспечить явный запрет доступа, который предотвращает любой доступ пользователя к файлам в каталоге. В некоторых реализациях можно управлять типами обращений к файлу. Реализации могут предоставлять опцию управления доступом, которая позволяет владельцу помечать файл как *разделяемый* или *заблокированный* (монопольно используемый). Разделяемые файлы позволяют осуществлять параллельный доступ к файлу нескольких пользователей в одно и то же время. Блокированный файл будет разрешать доступ к себе только одному пользователю в данный момент времени. Если файл доступен только по чтению, назначение его разделяемым позволяет группе пользователей параллельно читать его.

Эти средства управления доступом могут также использоваться, чтобы ограничить допустимые типы взаимодействия между серверами в КИС. Большое количество операционных систем в КИС могут ограничить тип трафика, посылаемого между серверами. Может не существовать никаких ограничений, что приведет к тому, что для всех пользователей будут

доступны ресурсы всех серверов. Политика КИС должна определить, какими типами информации необходимо обмениваться между серверами. На передачу информации, для которой нет необходимости совместного использования ее несколькими серверами, должны быть наложены ограничения.

Механизмы привилегий позволяют авторизованным пользователям игнорировать ограничения на доступ, легально обходить управление доступом, чтобы выполнить какую-либо функцию, получить доступ к файлу, и т.д. Механизм привилегий должен включать концепцию минимальных привилегий. Пользователь, авторизованный на выполнение функции резервного копирования, должен иметь доступ по чтению ко всем файлам, чтобы копировать их на резервные носители информации. Пользователю предоставляют привилегию обхода ограничения по чтению для всех файлов, чтобы он мог выполнить функцию резервного копирования. Чем более детальные привилегии могут быть предоставлены, тем больше будет гарантий, что пользователю не даны чрезмерные привилегии для выполнения им авторизованной функции. Например, пользователю, который должен выполнять функцию резервного копирования, не нужна привилегия обхода ограничения на запись в файлы, но механизмы привилегий, которые не обеспечивают такую точность, могут привести к предоставлению ему такой привилегии.

Типы механизмов защиты, которые могли бы быть использованы для обеспечения службы управления доступом:

− механизм управления доступом, использующий права доступа;

− механизм управления доступом, использующий списки управления доступом, профили пользователей и списки возможностей;

− управление доступом, использующее механизмы мандатного управления доступом;

− детальный механизм привилегий.

Конфиденциальность данных и сообщений.

Служба конфиденциальности данных и сообщений может использоваться, когда необходима секретность информации. Эта служба может включать в себя механизмы, связанные со службой управления доступом и шифрования. Если служба управления доступом будет обойдена, к файлу может быть осуществлен доступ, но информация будет все еще защищена, поскольку находится в зашифрованной форме. Очень трудно управлять неавторизованным доступом к трафику данных, когда он передается по сетевым каналам КИС. Многие пользователи КИС это осознают и понимают проблему. Использование шифрования сокращает риск какого-либо перехвата и чтения проходящих сообщений, делая их нечитаемыми для тех, кто может осуществить перехват.

Только авторизованный пользователь, который имеет правильный ключ, сможет расшифровать сообщение после его получения. Хорошая политика безопасности должна явно указывать пользователям типы информации, которые считаются критичными настолько, что для них требуется применение шифрования. Концептуальная политика безопасности организации может указывать широкие категории информации, которые должны быть обязательно защищены, в то время как политика безопасности конкретной КИС может детализировать определенные типы информации и определенные среды работы, например, ОС, для которых необходима защита при помощи шифрования. На каком бы уровне политики безопасности не предписывалось использование шифрования, решение о его применении должно быть принято лицом в руководстве корпорации, ответственным за защиту критической информации. Если в политике не указывается, какая информация подлежит шифрованию, то владелец данных полностью отвечает за принятие этого решения.

В криптографии применяются секретные или открытые ключи. Криптография секретных ключей основана на использовании единственного криптографического ключа, известного двум сторонам. Один и тот же ключ используется для шифрования и расшифровки данных. Примером может

служит алгоритм — Стандарт Шифрования Данных (DES) с секретным ключом, используемый в криптографической системе, которая может обеспечить конфиденциальность. DES-алгоритм может быть реализован аппаратными средствами ЭВМ, программным обеспечением, программируемым оборудованием или некоторой их комбинацией.

Криптография с открытыми ключами — форма криптографии, которая использует два ключа: открытый ключ и секретный ключ. Два ключа связаны, но имеют такое свойство, что по данному открытому ключу в вычислительном отношении невозможно получить секретный ключ. В криптосистеме с открытыми ключами каждая сторона имеет собственную пару из открытого и секретного ключей. Открытый ключ может быть известен любому лицу; секретный ключ хранится в тайне. Технология открытых ключей в форме цифровых подписей может также обеспечить целостность и контроль участников взаимодействия.

Типы механизмов безопасности, которые могут быть реализованы, чтобы обеспечить службу конфиденциальности сообщений и данных:

− технология шифрования файлов и сообщений,

− защита резервных копий на лентах, дискетах, и т.д.,

− физическая защита физической среды КИС и устройств, использование маршрутизаторов, которые обеспечивают фильтрацию для ограничения широковещательной передачи (или блокировкой, или маскированием содержания сообщения).

В целом существует значительное количество систем, позволяющих выполнять оценку свойств поступающей информации [12-15]. Для анализа таких систем используем критерии:

− архитектурные: о расширяемость; о наличие открытого кода; о наличие зависимости от других систем.

− функциональные: о тип обрабатываемой информации; о тип обнаруживаемых угроз; о работа с распределёнными системами; о используемые методы; о возможности учёта контекста.

К системам, выполняющим обнаружение аномалий во входящем потоке информации, относятся Snort.AD и Cerberus. Рассмотрим эти системы подробнее.

На рисунке 3 приведена структура системы Snort.AD [12]:

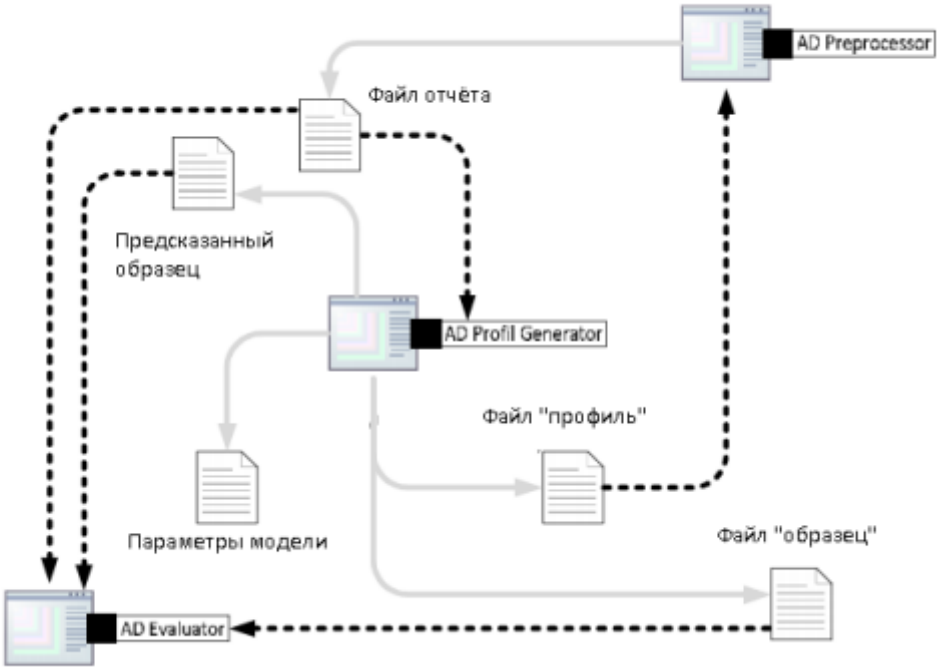

Рисунок 3 − Схема системы Snort.AD (Серая стрелка означает, что модуль записывает данные в файл, пунктирная – что модуль читает из файла)

Система состоит из препроцессора (AD Preprocessor – сбор данных о трафике и выдача предупреждений), генератора профилей (AD Profile Generator – прогнозирование трафика) и модуля оценки профиля (AD Evaluator – сравнение предсказанных данных с реальными). Препроцессор читает образец (предсказанные величины трафика) из файла «профиль» и генерирует тревогу, если текущее значение выходит за рамки допустимого (т. е. не лежит в пределах от минимума до максимума). Выполняется сбор следующих данных: число TCP-, UDP-, ICMP-пакетов (как общее число, так и число входящих и исходящих), число этих же пакетов из своей подсети, количество TCP-пакетов с флагами SYN/ACK, количество входящих и исходящих WWW-пакетов (под ними подразумеваются TCP-пакеты на стандартный порт 80), число входящих/исходящих DNS-пакетов (UDP на

53), количество ARP-запросов и ответов, количество не-TCP/IP пакетов, скорости трафика по всем этим составляющим трафика.

Основными ограничениями Snort.AD является то, что он не учитывает значимые компоненты контекста информации (пространство, идентификатор пользователя), а также анализирует исключительно сигнальную информацию в формате временных рядов и только информацию о сетевом трафике. Если вторая проблема может быть устранена с помощью разработки дополнительных модулей сбора и анализа информации, то первая порождает архитектурные проблемы в области интеграции данных с разных узлов КИП.

Система Cerberus [13], напротив, оптимизирован для распределённых систем и позволяет максимально учитывать контекст поступающей информации. Например, оценка достоверности аутентификации пользователя может быть разной в зависимости от контекста. Однако в Cerberus рассматривается только аутентификационная информация. Кроме того, Cerberus может разрешать или запрещать доступ к ресурсам в зависимости от статуса аутентификации, но не учитывает возможность конфликтов доступа.

Фреймворк ConSec [14] также рассматривает контекст в КИП, но защищает только коммуникационный процесс между компонентами системы.

Сведём рассмотренные системы в таблицу 1. В целом анализ существующих систем и фреймворков показывает, что целью их разработки является защита конфиденциальности и обеспечение высокой точности при аутентификации пользователей. При этом вопросы обеспечения доступности при большом количестве пользователей, которые легитимны, но пользуются разной степенью доверия, рассматриваются только в Snort в контексте противодействия DDoS атакам. Однако Snort имеет очень ограниченные возможности учёта контекста и работы в многопользовательских системах.

Таблица 1 − Системы обеспечения ИБ КИС

Критерии	**Системы**			
Функциональные:	Snort.AD	Cerberus	ConSee	Semantic security framework
тип информации	Только временные ряды	Аутентификационные данные и контекст	Аутентификационные данные и контекст	Аутентификационные данные и контекст
методы обработки	Математическая статистика	Логический вывод	?	Онтологии, логический вывод
Тип угроз	DoS, DDoS	НСД	НСД	НСД
распределённость	Нет	да	да	да
контекст	Не полностью	да	да	да
Архитектурные:				
открытый код	да	?		
расширяемость	да	?		
зависимости	нет	Gaia [71]		Smart-M3

Таким образом, систем и фреймворков, полностью соответствующих требованиям, не разработано. Тем не менее, значительное количество методов, используемых в этих системах и опубликованных в научной литературе, применимы для решения поставленных задач.

Вывод по первой главе

В первой главе были рассмотрены понятие корпоративной информационной системы и ее значение защиты в образовательной организации. Была изучена концепция информационной корпоративной информационной системы, описаны системы защиты корпоративных информационных систем.

Корпоративная информационная система – это открытая интегрированная система реального времени, автоматизирующая бизнес-процессы предприятия всех уровней и направлений деятельности, в том числе бизнес-процессы принятия управленческих решений.

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

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

Под защитой информации КИС понимается комплекс организационных, правовых и технических мероприятий по предотвращению угроз информационной безопасности и устранению их негативных последствий путем создания системы защиты информационных ресурсов КИС - СЗИ.

Система защиты информации (СЗИ) — совокупность механизмов, процедур и других управляющих воздействий, реализованных для сокращения риска, связанного с угрозой.

Систем и фреймворков, полностью соответствующих требованиям, не разработано. Тем не менее, значительное количество методов, используемых в этих системах и опубликованных в научной литературе, применимы для решения поставленных задач.

ГЛАВА 2. РАЗРАБОТКА РЕКОМЕНДАЦИЙ ПО ВЫБОРУ СРЕДСТВ ЗАЩИТЫ КОРПОРАТИВНОЙ ИНФОРМАЦИОННОЙ СИСТЕМЫ ГБПОУ «ЮЖНО-УРАЛЬСКИЙ ГОСУДАРСТВЕННЫЙ ТЕХНИЧЕСКИЙ КОЛЛЕДЖ»

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

В качестве объекта защиты было выбрано Государственное бюджетное профессиональное образовательное учреждение «Южно-Уральский государственный технический колледж». Местонахождение учебного корпуса: Политехнический комплекс: 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.

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.

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

Корпоративная информационная система состоит из пяти уровней:

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

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

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

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

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

− программные средства управления документооборотом;

− программные комплексы для ведения конструкторских работ (САПР);

− программные средства электронного офиса (MS Qffice);

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

− информационно-аналитические системы (Deductor).

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

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

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

Для управления образовательным процессом и обеспечения коммуникации между преподавателями и студентами колледжа (ЮУрГТК) используются различные информационные системы:

− система электронного документооборота (используется для обмена документами между участниками образовательного процесса);

− система электронного расписания (позволяет студентам и преподавателям получать доступ к расписанию занятий и изменениям в нем);

− система электронной почты (обеспечивает коммуникацию между преподавателями и студентами);

− система дистанционного обучения (позволяет студентам получать доступ к учебным материалам и заданиям в любое время и из любого места);

− система управления базами данных (используется для хранения и управления информацией о студентах, преподавателях и учебных материалах);

− 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.

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

В качестве типовых примеров угроз доступности информации в сервисах КИС могут выступать:

1. Целенаправленные деструктивные воздействия на КИС с помощью недостоверной или некорректной информации. В этом случае источником угрозы является пользователь КИС, который может быть, как легитимным, так и нелегитимным. Типовым примером реализации такой угрозы является атака «отказ в обслуживании» (DoS), и, в частности, атака распределённого отказа в обслуживании (DDoS), генерируемая сетями заражённых компьютеров (ботнетами) [99].

2. Нецеленаправленные воздействия на КИС в условиях поступления от множества пользователей заявок, которые не могут быть выполнены сервисами КИС в сроки, при которых актуальность заявок сохраняется. В этом случае источником угрозы является легитимный пользователь КИС. Пример реализации угрозы – исчерпание пропускной способности канала передачи данных при возникновении эффекта «flash crowd» [100].

3. Ошибочное восприятие сервисами КИС поступающих заявок. Эта угроза вероятна при использовании многомодальных средств человеко-машинного взаимодействия – при взаимодействии с сервисами с помощью речи, жестов, при распознавании образов на видео. Также угроза может реализоваться из-за ошибок в клиентском или серверном программном

обеспечении. Источник угрозы – программное обеспечение КИП. Обработка сервисами ошибочно воспринятых данных негативно сказывается на доступности сервисов для легитимных пользователей.

Таким образом, для обеспечения оптимального качества обслуживания пользователей в КИС необходимо совершенствование систем и разработка адаптивных методов защиты, учитывающих особенности условий функционирования.

Для спецификации угроз, актуальных для КИС, необходимо рассмотреть их возможные источники. Источники угроз систематизированы на рисунке 4.

Рисунок 4 − Классификация источников угроз

Угрозы, в свою очередь, классифицируются:

− по источнику;

− по аспекту ИБ (целостность, доступность, конфиденциальность);

− по целевому компоненту системы (АО, СПО, ППО).

Таким образом, угрозы можно свести в таблицу 2.

Таблица 2 − Угрозы КИС

Источник	Аспект	Цель	Угрозы	События риски
Оператор	Целостность	СПО	Ошибочные действия в административном интерфейсе	Утрата данных
Гость	Доступность	СПО	Неисполняемые запросы	Недоступность управления КТ для других пользователей
Нелегитимный пользователь	Целостность	ППО	Инъекция (SQL)	Утрата или модификация данных
	Доступность	ППО	Инъекция (XSS)	Недоступность административного интерфейса
	Доступность	АО, СПО, ППО (в зависимости от типа DDoS	DoS, DDoS	Недоступность интерфейсов для загрузки данных
	Конфиденциальность	ППО	Эксплуатация уязвимостей в аутентификации (недостаточная аутентификация, индексирование директорий, и т.п.	Кража идентификационных данных
Системное ПО	Доступность	ППО	Отказ	Невозможность работы сервиса
ПО сервиса	Доступность	ППО	Дефект	Некорректная работа сервиса
Нелегитимное ПО	Доступность	ППО, СПО, АО	Исчерпание программных или аппаратных ресурсов	Недоступность интерфейсов или сервиса в целом
	Целостность	ППО, СПО, АО	Несанкционированный доступ	Утрата данных
	Конфиденциальность	ППО	Несанкционированный доступ	Кража идентификационных данных
	Доступность, целостность, конфиденциальность	ППО	Организация каналов обмена информацией	Утрата, кража данных
АО	Доступность, целостность	ППО	Сбой электропитания	Невозможность работы сервиса, утрата данных

Продолжение таблицы 2

Сетевое АО	Доступность	ППО	Отказ	Недоступность интерфейсов
	Конфиденци-альность	ППО	Перехват трафика	Кража идентификационных данных
АО хранения данных	Доступность	ППО	Отказ	Невозможность работы сервиса
	Целостность	ППО	Отказ	Утрата данных
АО обработки данных	Доступность	ППО	Отказ	Невозможность работы сервиса

Следует отметить, что в значительном количестве случаев угрозы затрагивают сразу несколько компонентов системы и аспектов информационной безопасности. Такие угрозы назовём комплексными. При защите следует приоритетно рассматривать именно такие угрозы, так как они получают всё большее распространение в связи с ростом сложности защищаемых систем и являются более общим классом по отношению к частным угрозам.

Для проведения анализа уязвимостей корпоративной информационной системы ГБПОУ «Южно-Уральского государственного технического колледжа» наиболее оптимальным методом является разработка модели угроз. Необходимость разработки модели угроз регламентирована рядом нормативных документов, таких как:

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

2. Состав и содержание организационных и технических мер по обеспечению безопасности персональных данных при их обработке в информационных системах персональных данных (утверждены приказом Федеральной службы по техническому и экспортному контролю России (ФСТЭК России) от 18 февраля 2013г. No 21): «Меры по обеспечению

безопасности персональных данных реализуются, в том числе посредством применения в информационной системе средств защиты информации, прошедших в установленном порядке процедуру оценки соответствия, в случаях, когда применение таких средств необходимо для нейтрализации актуальных угроз безопасности персональных данных» [30].

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

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

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

− описание информационной системы;

− структурно-функциональные характеристики;

− описание угроз безопасности;

− модель нарушителя;

− возможные уязвимости;

− способы реализации угроз;

− последствия от нарушения свойств безопасности информации.

Для модели угроз изначально определяется глобальный параметр – уровень исходной защищенности. Определяется он один раз и не меняется от угрозы к угрозе. Чтобы определить уровень исходной защищенности (он же коэффициент исходной защищенности Y1) нужно для семи показателей

выбрать одно из значений, которое больше всего подходит для вашей системы.

Каждому значению соответствует высокий, средний или низкий уровень защищенности. Считаем какой процент у нас получился для показателей с разными значениями. Если «высокий» и «средний» набрали 70% и выше, то определяем средний уровень исходной защищенности (Y1 = 5), если нет, то – низкий (Y1 = 10).

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

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

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

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

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

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

– 0 – для маловероятной угрозы;

– 2 – для низкой вероятности угрозы;

– 5 – для средней вероятности угрозы;

– 10 – для высокой вероятности угрозы.

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

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

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

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

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

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

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

Следующий столбец – актуальность угрозы. Определяется по таблице правил отнесения угрозы безопасности ПДн к актуальной (таблица 3).

Таблица 3 – Правила отнесения угрозы безопасности ПДн к актуальной

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

В результате была разработана модель угроз для ГБПОУ «Южно-Уральского государственного технического колледжа», представленная в приложении 1. В модели угроз отражены все возможные угрозы корпоративной информационной системе образовательной организации, дана вероятностная оценка реализации угрозы и представлены возможные меры по исключению риска наступления данного события.

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

Разработка рекомендаций по выбору средств защиты корпоративной информационной системы образовательной организации является важным процессом.

При разработке рекомендаций, необходимо учесть следующие условия:

1. Прежде чем выбирать средства защиты, необходимо провести анализ уязвимостей и рисков в корпоративной информационной системе. Это поможет определить, какие угрозы могут возникнуть и какие меры защиты необходимы.
2. Разработать список требований к безопасности, которые должны быть удовлетворены выбранными средствами защиты. Это может включать в себя требования к шифрованию данных, контролю доступа, обнаружению вторжений и т.д.
3. Изучить рынок средств защиты и сравните различные продукты и услуги. Обратите внимание на их функциональность, надежность, стоимость и поддержку.
4. При выборе средств защиты учитывать их совместимость с другими системами и программным обеспечением, которые используются в образовательной организации.
5. Оценить стоимость выбранных средств защиты и их эффективность в защите корпоративной информационной системы. Выбранные средства защиты должны соответствовать бюджету и обеспечивать необходимую защиту.
6. Перед внедрением выбранных средств защиты необходимо провести тестирование и обучение сотрудников, чтобы убедиться в их эффективности и соответствии требованиям безопасности.

7. Регулярно обновлять и проверять выбранные средства защиты, чтобы убедиться в их эффективности и соответствии новым угрозам и требованиям безопасности.

Защита информации в корпоративных сетях – это комплекс мер по предотвращению утечки корпоративных данных, персональных данных (ПНд) сотрудников и обучающихся, отражение атак на ресурсы образовательной организации. Современные методы защиты включают в себя идентификацию и аутентификацию, разграничение прав доступа и управление доступом к данным, криптографию и создание межсетевых экранов.

Организация процедур комплексной защиты корпоративной информации в сетях осложнена использованием оборудования разных поколений и разных производителей, различных баз данных, локальных сетей (LAN).

Система корпоративной защиты информации должна отражать любые типы атак:

– попытки взлома хакерами;

– несанкционированный доступ к конфиденциальным данным, в т. ч. ПНд;

– заражение вредоносным программным обеспечением (ПО): вирусами, троянскими программами, «червями»;

– загрузке и установке шпионских программ, рекламного софта;

– спаму, фишинг-атакам;

– взлому сайтов (CMS), корпоративных групп в социальных сетях.

При этом применяемые средства и технологии защиты корпоративных данных не должны препятствовать нормальному функционированию информационных систем (ИС) образовательной организации, включая доступность данных из ИС для авторизованных пользователей. В целом, система комплексной защиты корпоративных данных должна отвечать требованиям:

– доступности для авторизованных, идентифицированных пользователей;

– целостностью, т.е. полноты и достоверности возвращаемых на запрос сведений;

– конфиденциальностью – предоставлением данных согласно уровню доступа пользователя.

Технология защиты корпоративных данных подразумевает:

– использование межсетевых экранов (программных и аппаратных) – современные решения позволяют настраивать VPN, интегрироваться с антивирусами;

– установку антивирусной защиты с закрытием почтовых шлюзов, прокси-серверов (зачастую одновременно применяется 2–3 антивирусные программы с различными методами обнаружения вредоносного ПО);

– настройку систем обнаружения атак (IDS);

– создание единой консоли управления информационной безопасности.

Комплексная защита корпоративной информации.

Современная система защиты корпоративных данных в сетях должна противодействовать случайным и преднамеренным атакам, внутренним и внешним источникам угрозы (направленным на данные, программы, аппаратуру, поддерживающую инфраструктуру).

Также не следует трактовать защиту корпоративных данных исключительно только как предотвращение несанкционированного доступа со стороны злоумышленников. Часто перед специалистами ставится задачи:

– при выборе оператора облачного сервиса, виртуального сервера (хостинг-провайдера) – отслеживать uptime сервера (объективно он не может быть равен 100%, однако для ответственных решений существует правило 4-х и ли 5-и девяток, т.е. доступности сервера в 99,99% или 99,999% времени), особенно если остановка его (сервера) работы может привести к серьезным потерям;

–устранение последствий технических сбоев, потерь данных в случае техногенных катастроф, случайного или умышленного нарушения правил эксплуатации информационной системы (ИС), при превышении расчетного числа запросов к БД, пропускной способности каналов связи и т.д.;

–устранения ошибок конфигурирования, топологии сети, отказов аппаратных или программных модулей, физического разрушения (износа) аппаратной части системы и т.п.

Однако настоящие проблемы являются, как правило, прозрачными и прогнозируемыми. В то время как попытки взлома, несанкционированного доступа потенциально более опасны, непредсказуемы.

1. Защита корпоративных данных от атак.

Самое узкое место в защите передачи информации – это белый IP адрес, через который передается и принимается информация. Большинство атак в сети Интернет направленно на выявление незащищенных портов на устройстве (далее Firewall (файрволл)), к которому привязан данный белый IP адрес.

Атакующий перебирает все популярные протоколы передачи информации (SSH, RDP, FTP, HTTP, SMTP и другие) и сканируя открытые порты устройства.

Найдя такие порты, злоумышленник начинает перебирать известные логины сотрудников образовательной организации и сопоставляя скомпрометированные пароли отправляя запросы на авторизацию на устройстве.

2. Доступ к информации в корпоративных системах.

Помимо защиты от атак извне необходим доступ к корпоративной информации образовательной организации сотрудников вне пределов периметра организации через сеть Интернет. Используя FTP-сервера, RDP подключение к рабочему компьютеру, мы просто упрощаем работу злоумышленника. Правильнее сегодня использовать VPN (Virtual Private Network) сети.

RDP подключение использует для соединения один порт устройства, и если удаленных сотрудников 10, 20, 100 – то нужно открыть 10, 20, 100 портов на файрволле. В случае организации подключения через VPN – открытый порт будет один.

3. Управление каналом Интернет при защите корпоративных данных.

Чем больше сотрудников в образовательной организации, работающих в сети Интернет, тем больше нагрузка на основной канал. А ширина канала Интернет всегда ограничена, да и сотрудник колледжа должен работать, а не сидеть в социальных сетях, развлекательных, игровых сайтах. Для этого вырабатываем правила использования сети Интернет внутри образовательной организации – идет градация сотрудников. Например, можно назначить три вида доступа:

- обычный – ограниченный: запрещены доступы к социальным сетям, сайтам типа YouTube*, rutube, игровым и т.д.;
- привилегированный – неограниченный доступ к сети Интернет, но через специальную систему фильтр;
- прямой доступ – доступ к сети интернет минуя все корпоративные системы защиты информации. Обычно такой доступ предоставляли системам корпоративной видеосвязи.

Большинство пользователей образовательной организации заходят на одни и те же сайты и каждый раз открывая одну и ту же страницу в Интернет создают дополнительную нагрузку на канал. В целях экономии трафика рекомендуется использовать прокси-сервер.

1. Фильтрация трафика в корпоративных сетях.

Пользователи через канал Интернет получают различную информацию – файлы, сообщения электронной почты и многое другое. Злоумышленник постарается прислать для взлома корпоративной сети вирус, троян, ссылку на фишинговый сайт. Необходимо фильтровать весь входящий и исходящий в единой общей точке.

5. Анализ данных.

В организации каждая служба (кадровая, служба безопасности и другие) хочет понимать, чем живет и дышит их сотрудник, какие сайты посещает, сколько времени сотрудник проводит в сети Интернет, отрываясь от основной работы. Поэтому работу сотрудника в сети Интернет необходимо тщательно анализировать.

Вышеперечисленные задачи всегда в определенный момент времени возникают перед службой ИТ и каждый начинает решать их по-своему. И если использовать разнообразные системы, то на их поддержку уйдет много времени и потребуется не один сотрудник. Но существуют комплексные решения управления и защиты интернет трафика, которые содержат в себе – программный файрвол, систему фильтрации трафика, интеграция с антивирусом для фильтрации входящего и исходящего трафика, прокси-сервер, VPN-сервер, систему обнаружения и предотвращения вторжений (IPS).

Примеры систем: Kerio Control, iDeco, UserGate, CheckPoint, Sophos UTM, FORTIGATE.

Наиболее доступными из решений являются Kerio, Ideco, UserGate. Решения Checkpoint, Sophos, Fortigate относятся к классу Enterprise. Большинство решений являются независимыми аппаратно-программными комплексами, что сказывается на их цене. Решения поддерживают интеграцию с большинством известных антивирусов, содержат мощный инструмент отчетности и анализа.

Не существует ПО, которое обеспечивало бы 100% уровень защиты. Более того, пользователь (системный администратор) зачастую не может повлиять на уязвимости в конкретном продукте (иначе как отказаться от его использования). Поэтому при выборе инструментов защиты корпоративных данных следует использовать ПО, уязвимости которого либо не несут пользователю ощутимой угрозы, либо их реализация с точки зрения злоумышленника бесполезна.

На что обращать внимание при выборе таких систем:

- функционал;
- требования к аппаратной части;
- юзабилити (удобство использования);
- возможность анализировать https трафик;
- работа без агентов;
- интеграция с существующим в образовательной организации антивирусом;
- возможность резать канал интернет на полосы;
- на возможность решения поставленных перед вами задач.

Перед внедрением необходимо тестовую версию продукта протестировать на ограниченном круге лояльных пользователей.

Наиболее действенные способы повышения безопасности от внешних угроз:

- межсетевой экран;
- организация демилитаризованной зоны;
- контроль и учет трафика сетевых подключений;
- антивирусное ПО, система защиты от вторжений;
- средства защиты от шпионских и DDoS-атак.

Для обеспечения безопасности информации ограниченного доступа должны применяться сертифицированные средства защиты информации. При наличии сетевого взаимодействия обязательны межсетевые экраны (МЭ).

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

Среди задач, которые решают межсетевые экраны, основной является защита сегментов сети или отдельных хостов от несанкционированного доступа с использованием уязвимых мест в протоколах сетевой модели OSI или в программном обеспечении, установленном на компьютерах сети.

Межсетевые экраны пропускают или запрещают трафик, сравнивая его характеристики с заданными шаблонами.

Функции межсетевого экрана включают в себя:

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

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

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

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

С точки зрения законодательства сертификат соответствия свидетельствует, что данное СЗИ разрешается применять для защиты сведений, относимых к охраняемой информации. Соответственно, в информационных системах (ИС), в которых обрабатываются такие сведения, необходимо применение сертифицированных СЗИ. Являющиеся для этого основой нормативные акты перечислены в таблице 4. Приведены приказы ФСТЭК, которые в свою очередь подзаконны соответствующим Федеральным Законам и Постановлениям Правительства, указанным в тексте документов.

Таблица 4 − Основные нормативные акты

Тип данных или информационного ресурса	**Нормативный акт**
Государственная тайна (ГТ)	Руководящие документы Гостехкомиссии России, закрытые документы
Персональные данные (ПДн)	Приказ ФСТЭК от 18 февраля 2013 г. №21
Государственные и муниципальные информационные системы (ГИС, МИС)	Приказ ФСТЭК от 11 февраля 2013 г. №17
Автоматизированные системы управления технологическими процессами (АСУ)	Приказ ФСТЭК от 14 марта 2014 г. №31
Значимые объекты критической информационной инфраструктуры (КИИ)	Приказ от 25 декабря 2017 г. №239
В отдельных случаях иная конфиденциальная информация	Руководящие документы Гостехкомиссии России, специальные нормативные акты

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

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

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

В классификации ФСТЭК России выделяют три основных типа межсетевых экранов: программные, аппаратные и программно-аппаратные.

Согласно ФСТЭК России, решения классифицируют по профилю защиты, который определяет степень их надежности и область применения. Важно выбирать подходящий межсетевой экран, исходя из специфики и требований сети.

Требования к МЭ устанавливает Приказ ФСТЭК от 09.02.2016 №9 (согласно информационному сообщению ФСТЭК от 28 апреля 2016 г. N 240/24/1986). Документ является закрытым, поскольку содержит информацию по защите ГТ. Из указанного информационного сообщения следует, что выделяются пять типов и шесть классов защищенности МЭ. В таблице 5 демонстрируется соотношение классов и типов защищаемой информации.

Таблица 5 − Соотношение классов и типов защищаемой информации

Класс защищенности МЭ / Тип и класс ИС		**6**	**5**	**4**	**3**	**2**	**1**
ГТ					■	■	■
ГИС	1 КЗ			■	■	■	■
	2 КЗ	■	■	■	■	■	■
	3 КЗ	■	■	■	■	■	■
	4 КЗ	■	■	■	■	■	■
ИСПДн	1 УЗ			■	■	■	■
	2 УЗ		■	■	■	■	■
	3 УЗ	■	■	■	■	■	■
	4 УЗ	■	■	■	■	■	■
АСУ	К1			■	■	■	■
	К2		■	■	■	■	■

	К3						
Значимые объекты КИИ	1 кат						
	2 кат						
	3 кат						
ИС ОП*	II класс						

*В совместном приказе ФСБ и ФСТЭК от 31 августа 2010 г. №416/489 разрешается использование МЭ, имеющих сертификат одного из ведомств (ФСТЭК не указан как обязательное).

Если ИС относится к нескольким типам, то принимаются более строгие меры защиты.

Типы МЭ различаются исходя из точки размещения:

- тип А — границе физической сети ИС или сегментов ИС;
- тип Б — внутри физической сети на логической границе ИС либо сегментов ИС;
- тип В — внутри физической сети на хосте;
- тип Г — внутри физической сети на web-сервере;
- тип Д — в АСУ ТП.

Брандмауэры типа А могут иметь только программно-техническое исполнение, а типа В — только программное. Во всех остальных случаях можно выбирать исполнение по своему усмотрению.

Для государственных учреждений есть отдельное требование — использовать IT-решения отечественного производства. Многие частные компании тоже переходят на такие инструменты по причине их высокой эффективности.

Оптимальное решение — Solar NGFW для обеспечения комплексной защиты корпоративных сетей крупного бизнеса, ведомственных предприятий и органов власти. Это надежная альтернатива иностранным межсетевым экранам. Инструмент удобен в эксплуатации, оснащен встроенным потоковым антивирусом и отлично интегрируется с другими

решениями. Система Solar NGFW — ключ к информационной безопасности вашей компании и главный барьер на пути киберпреступников.

Solar NGFW — программное средство для комплексной защиты сети крупного бизнеса с централизованным выходом в интернет. Помогает импортозаместить иностранные NGFW без снижения уровня защищенности и удобства использования:

1. Защита от атак на периметре сети и ее сегментация.

2. Самый быстрый виртуализированный межсетевой экран — до 20 Гбит.

3. Контроль приложений с помощью глубокого анализа пакетов (DPI).

4. Сигнатуры IPS от Solar JSOC — коммерческого SOC №1 в России.

5. Встроенный антивирус для защиты от вредоносного ПО и сайтов.

6. Интеграция с другими средствами защиты по протоколам ICAP и syslog.

Управление доступом в интернет:

1. Гибкие иерархические политики доступа пользователей к веб-ресурсам.

2. Категоризатор для блокирования доступа к нежелательному контенту.

3. Досье на сотрудника и интерактивные отчеты для анализа использования интернета.

4. Реверс-прокси для контроля доступа к внутренним веб-ресурсам: OWA, 1С и т.д.

5. Нативная интеграция с DLP-системой Solar Dozor для предотвращения утечек.

Принцип работы. Solar NGFW устанавливается в разрыв трафика и проверяет все проходящие через него пакеты данных. При этом механизмы защиты NGFW работают параллельно, но каждый по своим базам сигнатур и правил. Это обеспечивает комплексную проверку трафика на соответствие политике безопасности.

Рисунок 5 – Принцип работы

В Solar NGFW реализованы все необходимые механизмы для комплексной защиты корпоративной сети: межсетевой экран с трансляцией IP-адресов, система обнаружения и предотвращения вторжений, антивирус, а также система глубокого анализа пакетов для контроля приложений. Кроме того, в Solar NGFW есть компоненты для управления доступом к веб-ресурсам: категоризатор, веб-прокси, реверс-прокси и механизмы контентного анализа.

В межсетевом экране реализован механизм смены IP-адресов (NAT), позволяющий скрыть от злоумышленника внутреннюю топологию корпоративной сети и пресечь разведку:

- блокировка сетевых угроз (L3/L4 модели OSI);
- авторизация пользователей и приложений;
- маршрутизация трафика;
- скрытие IP-адресов объектов корпоративной сети.

В Solar NGFW встроена система обнаружения и предотвращения вторжений (IPS). Она позволяет быстро идентифицировать и остановить сложные сетевые атаки, которые могут быть пропущены межсетевым экраном.

Входящий трафик проверяется на совпадение с сигнатурами атак. Это обеспечивает обнаружение и блокировку запросов и данных, не соответствующих политике безопасности. Также фиксируются потенциально опасные аномалии трафика. Стандартные сигнатуры IPS дополняются уникальными сигнатурами от Solar JSOC — первого и крупнейшего коммерческого SOC в России (собственная разработка на базе Suricata; сигнатуры от SOC №1 в России; регулярное автоматическое обновление баз сигнатур; создание исключений по сетевым параметрам/ID сигнатур).

В Solar NGFW оснащен антивирусом от российской компании. Он в реальном времени проверяет входящий трафик и выявляет вредоносные программы самых разных типов.

Модуль интегрирован в систему комплексной параллельной проверки трафика, не требует дополнительной настройки и обновляется в автоматическом режиме:

- автоматический анализ файлов и ссылок;
- противодействие социальной инженерии;
- оценка безопасности сайтов в реальном времени;
- автоматическое обновление.

В Solar NGFW реализован собственный категоризатор веб-ресурсов. Он позволяет блокировать доступ к фишинговым, нежелательным и запрещенным с точки зрения закона или работы сайтам. База веб-ресурсов обновляется ежедневно.

Категоризатор разработан компанией «Ростелеком-Солар» и включен в базовую версию Solar webProxy. Для наполнения и классификации базы веб-ресурсов используются технологии машинного обучения и искусственного интеллекта.

На рисунке 6 представлено место Solar NGFW в ИТ-инфраструктуре.

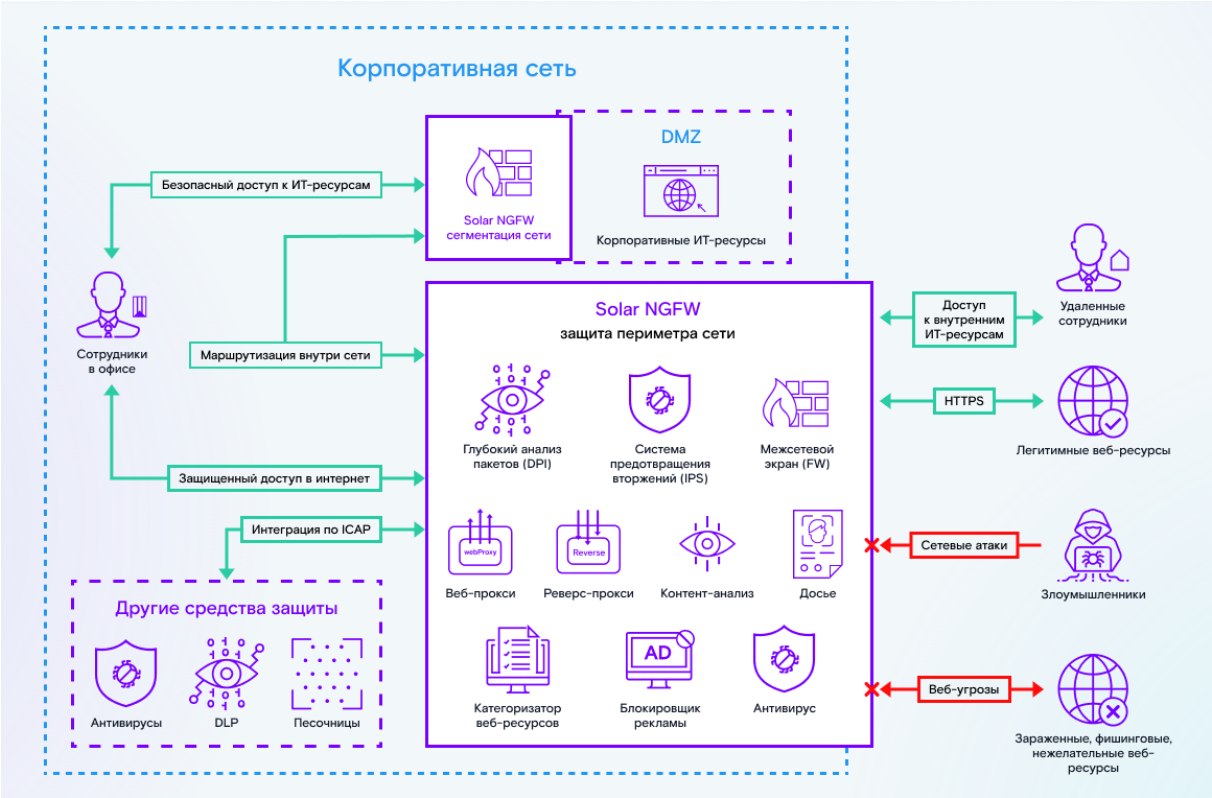

Рисунок 6 − Место Solar NGFW в ИТ-инфраструктуре

Основной сценарий применения Solar NGFW — установка на границе корпоративной сети для комплексной защиты от сетевых атак и управления доступом в интернет. Также возможно использование Solar NGFW для сегментации корпоративной сети и выделения DMZ для критически важных сервисов, например, сервера корпоративной почты. Встроенные функции SWG позволяют гибко управлять доступом в интернет для офисных сотрудников и доступом к внутренним веб-ресурсам организации для удаленных сотрудников.

Взаимодействие с Solar NGFW происходит через единую консоль управления, доступную из любого браузера. Она устроена как ситуационный центр и позволяет оперативно оценить обстановку и выделить приоритетные направления работы. Рутинные операции максимально автоматизированы. Для использования продукта не требуется проходить сложное обучение.

Окно программы представлено на рисунке 7.

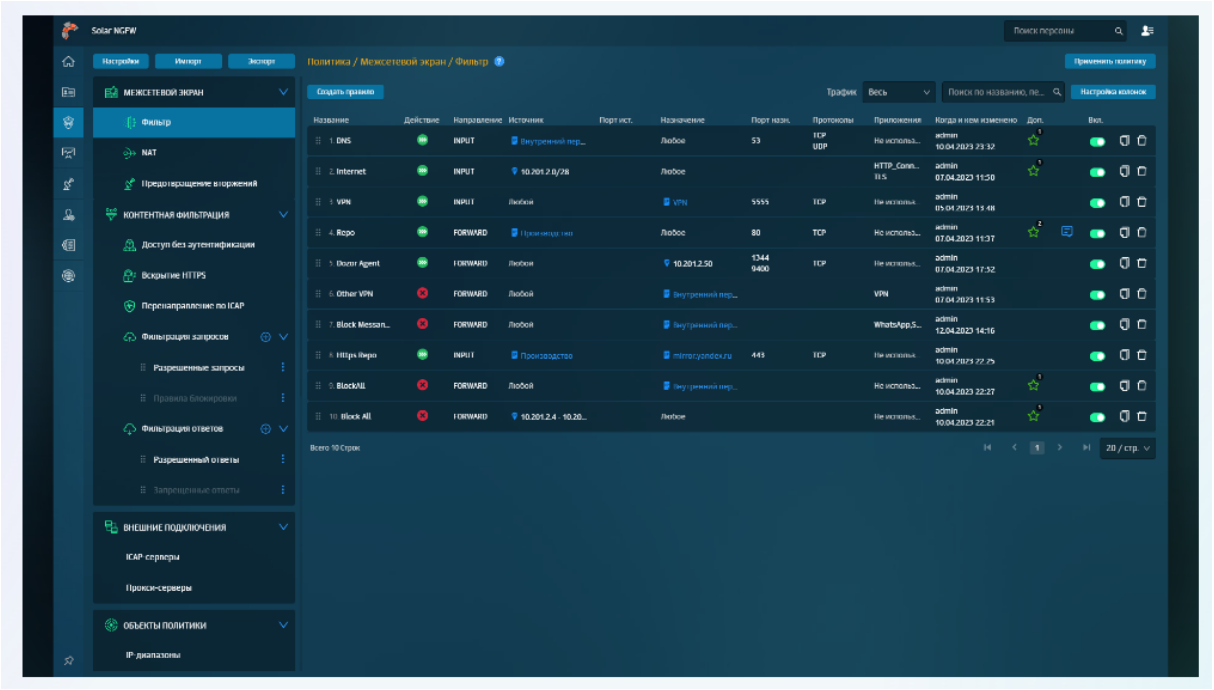

Рисунок 7 – Окно программы Solar NGFW

Таким образом корпоративную информационную систему образовательной организации нужно защищать в обязательном порядке. Межсетевой экран уменьшит вероятность вторжения извне, позволит установить ограничения на использование определенных программ сотрудниками, обеспечит безопасную передачу данных по FTP и прочим протоколам. Применение сертифицированного межсетевого экрана рекомендуется образовательным учреждениям, для которых важно отслеживать работу персонала и не допускать использование «непрофильных» программ и сайтов. При этом лучше установить аппаратно-программный брандмауэр, чтобы дополнительно не нагружать рабочие компьютеры.

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

В комплекс рекомендаций по выбору средств защиты корпоративной информационной системы входили анализ нормативно-правовых требований действующего законодательства и анализ угроз

образовательной организации. В результате были разработаны рекомендации по выбору средств межсетевого экранирования, в которые вошли ряд критериев, учитывающие специфику и цели образовательной организации, а также экспертная оценка, которая позволяет выбрать оптимальный межсетевой экран для образовательной организации.

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

В экономическую оценку вошли:

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

В обследование информационных систем входило:

– аудит документов, обследование помещений, сети и компьютеров;

– разработка модели угроз.

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

Согласно прайс-листу, цена на Solar NGFW на 2023 год составит за 1 год – 214 500 руб. (таблица 6).

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

Таблица 6 – Прайс-лист на Solar NGFW

Позиция	Стоимость за 1 год, руб.	Примечание
Аппаратная платформа Solar NGFW	100000	Цена с НДС 18%
Приобретение права на использование Solar NGFW	114500	НДС не облагается

В результате была составлена таблица расчёта стоимости защиты корпоративной информационной системы образовательной организации (таблица 7).

Таблица 7 – Расчёт стоимости защиты корпоративной информационной системы образовательной организации

№	Наименование товаров и услуг	Цена, руб.	Количество	Стоимость, руб.
1	*2*	*3*	*4*	*5*
I	ОБСЛЕДОВАНИЕ ИНФОРМАЦИОННЫХ СИСТЕМ			
1.1	Проведение обследования (аудит документов, обследование помещений, сети и компьютеров)	4 000	1	4 000
1.2	Разработка модели угроз	5 450	1	5 450
				9 450
II	ВНЕДРЕНИЕ МЕЖСЕТЕВОГО ЭКРАНИРОВАНИЯ В ОБРАЗОВАТЕЛЬНУЮ ОРГАНИЗАЦИЮ			
2.1	Аппаратная платформа Solar NGFW	100 000	1	100 000
2.2	Приобретение права на использование Solar NGFW	114 500	1	114 500
III	ОПЛАТА СИСТЕМНОГО АДМИНИСТРАТОРА			
3.1	Настройка, управление и мониторинг межсетевого экрана	35 000	*входит в ежемесячную оплату труда*	35 000
				258 950

В случае выявления нарушения в области информационной безопасности образовательной организации предусмотрена уголовная, административная, дисциплинарная и гражданская ответственность (таблица 8), которая может применяться в отношении организации, руководителя организации, подразделения или виновного работника [29].

Таблица 8 – 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 8

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

Продолжение таблицы 8

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
		защиты информации или без таковой
Статья 13.13 КоАП. Незаконная деятельность в области защиты информации	Занятие видами деятельности в области защиты информации (за исключением информации, составляющей государственную тайну) без получения в установленном порядке специального разрешения (лицензии), если такое разрешение (такая лицензия) в соответствии с федеральным законом обязательно (обязательна)	влечет наложение административного штрафа на граждан в размере от пятисот до одной тысячи рублей с конфискацией средств защиты информации или без таковой; на должностных лиц - от двух тысяч до трех тысяч рублей с конфискацией средств защиты информации или без таковой; на юридических лиц - от десяти тысяч до двадцати тысяч рублей с конфискацией средств защиты информации или без таковой

Продолжение таблицы 8

Статья 13.14 КоАП. Разглашение информации с ограниченным доступом	Разглашение информации, доступ к которой ограничен федеральным законом (за исключением случаев, если разглашение такой информации влечет уголовную ответственность), лицом, получившим доступ к такой информации в связи с исполнением служебных или профессиональных обязанностей	влечет наложение административного штрафа на граждан в размере от пяти тысяч до десяти тысяч рублей; на должностных лиц - от сорока тысяч до пятидесяти тысяч рублей или дисквалификацию на срок до трех лет; на юридических лиц - от ста тысяч до двухсот тысяч рублей
Дисциплинарная ответственность		
Статья 90 ТК РФ	Ответственность за нарушение норм, регулирующих обработку и защиту персональных данных работника	
Статья 192 ТК РФ	Дисциплинарные взыскания	
за совершение дисциплинарного проступка работодатель имеет право применить дисциплинарные взыскания: замечание, выговор, увольнение по соответствующим основаниям.		

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

Таким образом максимальный штраф, который может получить образовательная организация за нарушения в области информационной безопасности составит 370 000 руб. Дополнительно возможна конфискация средств защиты, приостановление или прекращение обработки персональных данных.

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

Для расчета экономической эффективности разработанных рекомендаций выбора средств защиты корпоративной информационной

системы необходимо суммарную её стоимость сравнить со стоимостью возможного ущерба со стороны регуляторных рисков (рисунок 8).

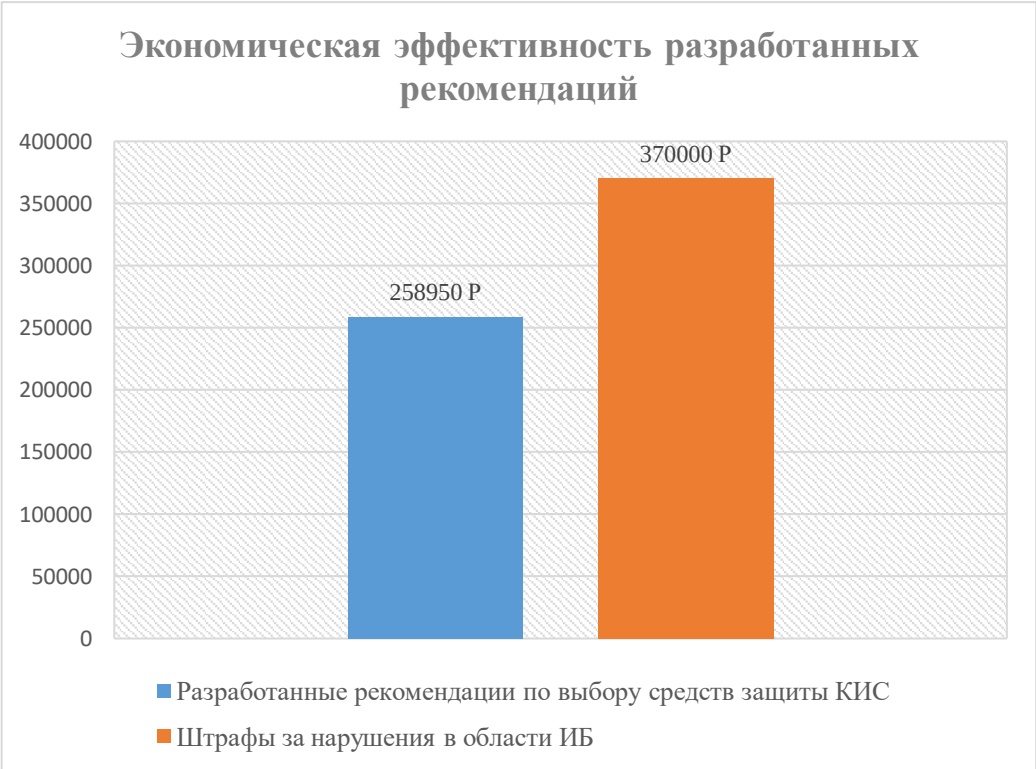

Рисунок 8 – Экономическая эффективность разработанных рекомендаций

В результате сравнения экономическая эффективность разработанных рекомендаций составила 111 050 руб. Учитывая данный показатель, можно сделать вывод, что реализация данного проекта экономически эффективна.

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

Вывод по второй главе

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

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

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

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

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

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

Наиболее действенные способы повышения безопасности от внешних угроз: межсетевой экран; организация демилитаризованной зоны; контроль и учет трафика сетевых подключений; антивирусное ПО, система защиты от вторжений; средства защиты от шпионских и DDoS-атак.

В качестве межсетевого экрана было выбрано программное средство Solar NGFW.

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

На внедрение разработанных рекомендаций образовательная организация потратит 258950 рублей, а стоимость возможного ущерба за нарушения в области информационной безопасности составят 370 000 рублей. В результате сравнения данных показателей экономическая эффективность разработанных рекомендаций составила 111 050 рублей.

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

ЗАКЛЮЧЕНИЕ

Выбор средств защиты корпоративной информационной системы образовательной организации требует тщательного анализа и планирования, чтобы обеспечить эффективную защиту от угроз и соответствие требованиям безопасности.

Для эффективной защиты корпоративной информационной системы необходимо провести анализ уязвимостей и рисков, определить требования к безопасности, изучить рынок средств защиты, учитывать совместимость, оценивать стоимость и эффективность, проводить тестирование и обучение сотрудников, а также регулярно обновлять и проверять выбранные средства защиты.

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

В результате анализа было выявлено, что корпоративная информационная система ГБПОУ «ЮУрГТК» имеет объективные, субъективные и случайные уязвимости. Наиболее оптимальным средством защиты корпоративной информационной системы для ГБПОУ «ЮУрГТК» является межсетевой экран за счёт его разнообразных функциональных возможностей.

В разработанных рекомендациях представлены наиболее действенные способы повышения безопасности от внешних угроз: межсетевой экран; организация демилитаризованной зоны; контроль и учет трафика сетевых подключений; антивирусное ПО, система защиты от вторжений; средства защиты от шпионских и DDoS-атак.

В качестве межсетевого экрана было выбрано программное средство Solar NGFW.

На внедрение разработанных рекомендаций образовательная организация потратит 258950 рублей, а стоимость возможного ущерба за нарушения в области информационной безопасности составят 370 000 рублей. В результате сравнения данных показателей экономическая эффективность разработанных рекомендаций составила 111 050 рублей.

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

Данное утверждение подтверждается в результате экономической оценки эффективности рекомендаций по выбору средств защиты корпоративной информационной системы образовательной организации ГБПОУ «ЮУрГТК». В данную оценку вошли расчет стоимости внедрения межсетевого экранирования для защиты корпоративной информационной системы образовательной организации и сравнение со стоимостью возможного ущерба со стороны регуляторных рисков. В результате сравнения экономическая эффективность разработанных рекомендаций составила 110 230 руб. Учитывая данный показатель, можно сделать вывод, что реализация данного проекта экономически эффективна.

Результаты исследования рекомендуется использовать в практической деятельности образовательных организаций среднего профессионального образования с целью повышения эффективности защиты корпоративной информационной системы.

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

СПИСОК ИСПОЛЬЗОВАННЫХ ИСТОЧНИКОВ

1. Автоматизированные системы. Защита от несанкционированного доступа к информации. Классификация автоматизированных систем и требования по защите информации [Электронный ресурс]: [руководящий документ ФСТЭК от 30.05.1992 г., с ред. от 09.12.2022 г.]. – Режим доступа: https://fstec.ru. Дата обращения: 15.09.2023.

2. Актаева А.У. Анализ проблем проектирования и внедрения информационных систем в вузах [Электронный ресурс] // Международный журнал «Программные продукты и системы». – 2009. – № 3. – Режим доступа: http://swsys.ru/index.php?page=article&id=2323(дата обращения: 16.10.2023.)

3. 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.

4. 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: 20.10.2023.

5. 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.

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

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

8. Государственный реестр сертифицированных средств защиты информации // reestr.fstec.ru [Электронный ресурс]. – URL: https://reestr.fstec.ru/reg3 (дата обращения: 05.11.2023).

9. Динмухаметов Р. Р. Методы защиты конфиденциальной информации в корпоративных информационных системах / Р.Р. Динмухаметов // «Наука. Образование. Инновации: современное состояние актуальных проблем». Сборник научных трудов по материалам XXIII Международной научно-практической конференции (г.-к. Анапа, 12 января 2024 г.). – Анапа: Изд-во «НИЦ ЭСП» в ЮФО, 2024. – С. 115-120.

10. Защита информационных систем // irsural [Электронный ресурс]. – URL: https://irsural.ru/nashi-uslugi/zashita-konfidecialnoi-informacii/zashita-informacionnyh-sistem/ (дата обращения: 15.11.2023).

11. Защита корпоративной информации. – URL: https://integrus.ru/blog/it-decisions/zashhita-korporativnoj-informatsii.html (дата обращения: 15.11.2023).

12. Идентификация (информационные системы) // Wikipedia [Электронный ресурс]: – URL: https://ru.wikipedia.org/wiki/Идентификация (информационные системы)/ (дата обращения: 15.11.2023).

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

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

15. Межсетевой экран // Wikipedia [Электронный ресурс]: – URL: https://ru.wikipedia.org/wiki/Межсетевой_экран (дата обращения: 15.11.2023).

16. Межсетевой экран. – URL: https://rt-solar.ru/products/solar_ngfw/blog/3408/#:~:text=%D0%9C%D0%B5%D0%B6

%D1%81%D0%B5%D1%82%D0%B5%D0%B2%D0%BE%D0%B9%20%D1%8D%D0%BA%D1%80%D0%B0%D0%BD%20(%D0%9C%D0%AD)%20%E2%80%93%20%D0%BE%D0%B4%D0%BD%D0%BE,%D0%BF%D0%BE%D1%81%D1%80%D0%B5%D0%B4%D1%81%D1%82%D0%B2%D0%BE%D0%BC%20%D1%81%D1%82%D0%B0%D0%BD%D0%B4%D0%B0%D1%80%D1%82%D0%BD%D1%8B%D1%85%20%D0%B8%20%D0%BA%D0%BE%D0%BC%D0%BF%D0%BB%D0%B5%D0%BA%D1%81%D0%BD%D1%8B%D1%85%20%D0%B8%D0%BD%D1%81%D1%82%D1%80%D1%83%D0%BC%D0%B5%D0%BD%D1%82%D0%BE%D0%B2 (дата обращения: 15.11.2023).

17. Межсетевые экраны – виды и особенности // smart-soft.ru [Электронный ресурс]. – URL: https://www.smart-soft.ru/blog/mezhsetevye-ekrany-vidy/ (дата обращения: 05.12.2023).

18. Межсетевые экраны, сертифицированные ФСТЭК. – URL: https://www.vistlan.ru/info/blog/obzory-tovarov/mezhsetevye-ekrany-sertifitsirovannye-fstek/ (дата обращения: 15.11.2023).

19. Методика оценки угроз безопасности информации [Электронный ресурс]: [методический документ ФСТЭК: от 05.02.2021 г.]. - Режим доступа: https://docs.cntd.ru (дата обращения: 20.11.2023).

20. 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: 10.11. 2023).

21. О стратегии национальной безопасности Российской Федерации [Электронный ресурс]: [указ президента РФ от 02.07.2021 № 400]. – Режим доступа: www.consultant.ru. Дата обращения: 10.11. 2023.

22. 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: 10.11. 2023.

23. 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: 10.11. 2023.

24. 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: 20.11.2023.

25. 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: 10.11. 2023.

26. 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: 20.10.2023.

27. 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: 20.11.2023.

28. Проблемы защиты информации на предприятии // rtmtech.ru [Электронный ресурс]. – URL: https://it-cube39.ru/news/137654/ (дата обращения: 05.11.2023).

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

30. Программно-аппаратная защита информации // searchinform [Электронный ресурс]. – URL: https://searchinform.ru/services/outsourceib/zaschita-informatsii/programmno-apparatnaya/ (дата обращения: 15.10.2023).

31. Профили защиты межсетевых экранов [Электронный ресурс]: [методический документ ФСТЭК РФ: от 12.09.2016 г.]. - Режим доступа: https://fstec.ru. Дата обращения: 05.12.2023.

32. 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: 05.12.2023.

33. 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: 20.12.2023.

34. Солончук Т. А. Корпоративные информационные системы в управлении образовательным учреждением // Современные тенденции в экономике и управлении: новый взгляд. 2011. №11-2. URL: https://cyberleninka.ru/article/n/korporativnye-informatsionnye-sistemy-v-upravlenii-obrazovatelnym-uchrezhdeniem (дата обращения: 03.12.2023).

35. 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: 10.12.2023.

36. Трояны удаленного доступа (RAT) – что это такое? // it-cube39.ru [Электронный ресурс]. – URL: https://it-cube39.ru/news/137654/ (дата обращения: 20.12.2023).

37. 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.

38. 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: 20.12.2023).

39. Фишинг // rt-solar.ru [Электронный ресурс]. – URL: https://rtsolar.ru/products/solar_dozor/blog/2844/ (дата обращения: 20.12.2023).

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

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

42. 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.

43. 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.

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

45. 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: 20.12.2023).

ПРИЛОЖЕНИЕ

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 каналам побочных электромагнитных излучения и наводок (ПЭМИН)	Маловероятна	Низкая	Низкая	Неактуальная		
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, уничтожение информации	Маловероятна	Низкая	Низкая	Неактуальна		Контролируемая зона для организации технической защиты конфиденциальной информации с ограничением доступа посторонних лиц; Ответственность за сохранность конфиденциальной информации и ее носителей в должностных инструкциях сотрудников
2.1.4 Вывод из строя узлов ПЭВМ, каналов связи	Низкая вероятность	Средняя	Низкая	Неактуальная		Контролируемая зона для организации технической защиты конфиденциальной информации с граничением доступа посторонних лиц; Ответственность за сохранность конфиденциальной информации и ее носителей в должностных инструкциях сотрудников
2.1.5 Несанкционированный доступ к информации при техническом	Маловероятна	Низкая	Низкая	Неактуальна		Ремонт допущенными сотрудниками учреждения; Технологический процесс

обслуживании узлов ПЭВМ						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 только администратору ; Настройка средств защиты	Инструктаж пользователей в части запрета каких-либо действий в отношении средств защиты
2.3.4 Выход из строя программно-аппаратных средств	Низкая вероятность	Средняя	Низкая	Неактуальна	Резервное копирование информации	
2.3.5 Сбой системы электроснабжения	Маловероятна	Низкая	Низкая	Неактуальна	Использование источников бесперебойного питания для серверов	
2.3.6 Стихийное бедствие	Маловероятна	Низкая	Низкая	Неактуальна	Пожарная сигнализация	Инструкция по действиям в случае возникновения нештатной ситуации
2.4 Угрозы преднамеренных действий внутренних нарушителей						
2.4.1 Доступ к информации, модификация, уничтожение лицами, не допущенными к ее обработке	Средняя вероятность	Средняя	Средняя	Актуальна		Инструктаж пользователей в части необходимости блокировки рабочих компьютеров в случае возможности просмотра информации людьми, не допущенными к данным сведениям; Парольная система доступа; Разграничение

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