МИНИСТЕРСТВО НАУКИ И ВЫСШЕГО ОБРАЗОВАНИЯ РОССИЙСКОЙ ФЕДЕРАЦИИ
федеральное государственное бюджетное образовательное учреждение
высшего образования
«Тольяттинский государственный университет»

Институт математики, физики и информационных технологий
(наименование института полностью)

Кафедра «Прикладная математика и информатика»
(наименование)

09.04.03 Прикладная информатика
(код и наименование направления подготовки)

Информационные системы и технологии корпоративного управления
(направленность (профиль))

ВЫПУСКНАЯ КВАЛИФИКАЦИОННАЯ РАБОТА (МАГИСТЕРСКАЯ ДИССЕРТАЦИЯ)

на тему Методы управления процессами информационной безопасности для обеспечения защиты информации корпоративной информационной системе

Студент А.Д. Дёмин
(И.О. Фамилия) (личная подпись)

Научный руководитель канд.пед.наук, доцент, О.М. Гущина
(ученая степень, звание, И.О. Фамилия)

Тольятти, 2021 г.

Оглавление

Введение

Актуальность темы выпускной квалификационной работы определяется обострением проблем информационной безопасности (ИБ) в условиях интенсивного совершенствования технологий и инструментов защиты данных. Об этом свидетельствует рост нарушений информационной безопасности, влекущих за собой необратимые последствия.

Совершенствование системы информационной безопасности на предприятиях, фирмах и организациях предприятиях очень важно в современном мире.

Успех современного предприятия и его развитие в условиях острой конкуренции в значительной степени зависят от применения информационных технологий, и как правило, от эффективных мер защиты ценной информации.

Под системой обеспечения информационной безопасности (ИБ) понимается совокупность организационных и инженерно-технических решений, направленных на защиту информационных ресурсов предприятия.

Для осуществления защиты информации на предприятиях должна быть сформирована политика информационной безопасности – определенный свод правил и нормативных документов, регламентирующих действия сотрудников по обеспечению безопасности, так же описывающие программные средства для защиты информации.

Конечная цель разработки политики информационной безопасности – обеспечить целостность, доступность и конфиденциальность для каждого информационного ресурса в процессе управления информационной безопасностью.

С помощью политики информационной безопасности мероприятия будут направлены на минимизацию рисков утечки информации на предприятии, а также для устойчивого функционирования информационной структуры предприятия и грамотных управленческих решений руководством

при управлении информационной безопасностью в корпоративной информационной системе. Нарушение политики ИБ и отсутствие современной, правильно выстроенной системы обеспечения безопасности в организации может привести к финансовым потерям, к потере важной информации, к большим издержкам материального характера, может нанести ущерб для имиджа предприятия, поэтому необходимо уделять пристальное внимание вопросам информационной безопасности.

Цель работы заключается в анализе управления информационной безопасностью для обеспечения защиты информации в ООО «Товаротранспортная компания».

Объект исследования – система информационной безопасности.

Предметом исследования является – методы и способы управления процессами информационной безопасности для обеспечения защиты информационных ресурсов.

Гипотеза исследования состоит в том, что предложенные мероприятия повысят уровень информационной безопасности на предприятии.

Реализация поставленной цели в выпускной квалификационной работе потребовала постановки и последовательного решения следующих взаимосвязанных задач:

- раскрыть понятие и задачи информационной безопасности;
- дать характеристику управлению процессами информационной безопасности;
- рассмотреть контроль и методы обеспечения информационной безопасности;
- провести анализ защиты данных в ООО «Товаротранспортная компания»;
- на основе методов управления информационной безопасностью, разработать методику анализа программного обеспечения с целью обнаружения возможности возникновения угроз;
- разработать комплекс программно-аппаратных средств обеспечения

информационной безопасности ООО «Товаротранспортная компания»;

- проанализировать риски и оценить их для эффективного управления информационной безопасностью;
- произвести расчёт показателей экономической эффективности проекта.

Теоретическая значимость исследования состоит в реализации комплексного подхода при разработке политики информационной безопасности в компании.

Новизна исследования заключается в том, что на основе практического опыта, разработана новая методика анализа программного обеспечения с целью определения возможности возникновения актуальных угроз при обеспечении информационной безопасности, которая усовершенствует существующие мероприятия по управлению процессами информационной безопасности.

На защиту выносятся:

- методика анализа программного обеспечения с целью обнаружения возможности возникновения угроз процессам информационной безопасности;
- комплекс программно-аппаратных средств, то есть внедрение мер по обеспечению защиты информации на предприятии;
- обоснование эффективности внедрения комплекса мер по защите ценной информации на предприятие ООО «Товаротранспортная компания».

Практическая значимость работы определяется тем, что результаты исследования могут применяться на предприятии для повышения уровня защиты информации.

Магистерская диссертация состоит и введения, трёх глав и заключения, изложенных на 109 страницах, а также списка использованной литературы (45 источников).

Глава 1 Теоретические аспекты управления процессами информационной безопасности

1.1 Понятие и задачи информационной безопасности на предприятии

Процесс управления информационной безопасностью входит в сферу компетенции общей информационной безопасности, задачей которой является обеспечение сохранности информации. Сохранность означает защищенность от известных рисков и, по возможности, уклонение от неизвестных рисков. Инструментом обеспечения этого является безопасность [35].

Благодаря достижениям научно-технического прогресса сегодня можно автоматизировать любые процессы. При этом не имеет значения область деятельности человека. После того как «появились автоматизированные системы обработки сведений, подвергся существенным изменениям формат их хранения и дальнейшего использования» [7].

Именно это стало причиной, по которой общество столкнулось с проблемой защиты данных, их хранения, использования. Также проблемным аспектом выступает обеспечение надлежащего уровня безопасности информации.

Под понятием информационная безопасность подразумевается защищенность сведений от целенаправленных или случайных воздействий. Такие воздействия могут быть естественными или искусственными. Они способны нанести огромный ущерб всем участникам информационных взаимоотношений. В частности, могут навредить владельцам сведений, пользователям.

Цель формирования полноценной системы безопасности сведений для защиты компании состоит в следующем:

– сформировать оптимальные условия для бесперебойной работы системы;

– обеспечить надлежащий уровень защиты жизни и здоровья работников;
– обеспечить эффективную защиту своей безопасности;
– предупредить риск кражи денег, материальных ценностей, искажения, распространения сведений конфиденциального характера. Также важно предотвратить порчу или уничтожение имущества. Важной задачей выступает обеспечение стабильной деятельности.

Процесс обеспечения безопасности компании базируется на принципах защиты сведений. Он подразумевает постоянное совершенствование защитных функций. Это связано с тем, что данная область все время развивается, улучшается. Защитные системы, которые были созданы всего несколько лет назад, быстро становятся неэффективными. С каждым годом повышается риск того, что злоумышленники взломают их [18].

Именно по этой причине система безопасности любой организации должна все время улучшаться. Можно выделить несколько принципов, на которые следует опираться в ходе формирования и модернизации рассматриваемых систем. К ним относятся:

– защита от атак злоумышленников;
– обеспечение надлежащего уровня безопасности недавно созданных видов информационных ресурсов;
– обеспечение доверенных взаимоотношений в информационном пространстве между всеми участниками (аутентификация, идентификация).

Управление информационной безопасностью тесно взаимосвязана с непрерывностью бизнес-процессов. Не принимая необходимых мер и плана по управлению информационной безопасности чревато последствиями различного рода, в плоть, до остановки непрерывности бизнес-процесса. Это потеря репутации и огромные убытки. Поэтому предприятие должно разработать подробные план (мероприятия), устанавливающие способы

управления в условиях инцидента и обеспечения непрерывности бизнеса и информационную безопасность.

Ключевое решение на мой взгляд, при разработке эффективного подхода для решения проблем при построении процесса управления информационной безопасностью, для осуществления эффективных управленческих решений в отношении обеспечения информационной безопасностью для построения эффективных мер защиты. Такое решение – это разработка политики информационной безопасности, так как она решает ключевую задачу, как комплексность. Так же необходимо отметить, что создание и внедрение политики информационной безопасности является методикой решения актуальных вопросов по обеспечению информационной безопасности.

В любой компании под политикой информационной безопасности понимается формирование главных задач и целей защиты сведений. Также создаются специальные правила, нормы, методы в сфере информационной безопасности. Аналогичные «приемы, принципы и средства формируются в области обеспечения безопасности данных в компании на организационном, технологическом, процедурном уровне» [31].

Главная цель рассматриваемой политики – это защита всех объектов информационных взаимоотношений. Она обеспечивается от вероятного нанесения ущерба. Он может быть физическим, моральным или другим, причиняться случайно или целенаправленно. Другой целью является защита носителей данных, процессов их обработки, хранения, передачи. Также необходимо сводить к минимуму степень различных рисков [21].

Помимо этого, к основным целям информационной безопасности компании относятся следующие:

- обеспечение надлежащей защиты информации фирмы;
- обеспечение надлежащей защиты конфиденциальных данных (сюда относятся данные работников компании и клиентов);
- веб-ресурсы, автоматизированные сети должны в полной мере

отвечать существующим стандартам защиты данных;

– обеспечение надлежащей защиты имущества компании.

Достижение обозначенных выше целей возможно путем разрешения таких задач:

– необходимо вовремя выявлять, изучать, оценивать, прогнозировать источники угроз данным компании. Также важно анализировать факторы, которые могут привести к нанесению ущерба участникам информационных взаимоотношений. Следует сформировать механизм быстрого реагирования на угрозы информационной безопасности;
– сформировать оптимальные условия для того, чтобы свести к минимуму наносимый ущерб. Чаще всего его причиной являются противозаконные действия юридических лиц и физических лиц. Необходимо устранить последствия нарушения безопасности данных;
– обеспечить надлежащий уровень защиты от посторонних людей и юридических лиц, которые могут вмешаться в процесс работы информационной системы. Важно, чтобы только пользователи, прошедшие регистрацию, имели доступ к информации компании;
– дифференцировать доступ пользователей к различным ресурсам, например, программным, информационным и прочим. Иными словами, следует предупредить несанкционированный доступ к системе безопасности;
– обеспечить аутентификацию пользователей, которые являются участниками информационного взаимодействия;
– обеспечить защиту от противозаконной модификации применяемых программных продуктов. Также необходимо создать эффективную защиту системы от воздействия вредоносных программ (вирусов);
– обеспечить надлежащую защиту сведений, доступ к которым ограничен. Важно предупредить их утечку в процессе обработки,

хранения и других операций с такими данными;

– применение современных криптографических методов защиты сведений.

Решить указанные выше задачи можно с помощью таких правил:

– важно учитывать все сведения, которым необходимо обеспечить защиту (например, данные о работниках компании и клиентах);
– строго учитывать все действия работников предприятия, которые занимаются обслуживанием программно-технических средств в компании;
– важно, чтобы все работники компании придерживались норм, обозначенных в ее документации;
– каждый работник несет ответственность за свои действия в пределах должностных обязанностей;
– следует использовать современные методы защиты ресурсов системы. Необходимо обеспечить постоянную техническую поддержку их применения, добиться непрерывности протекания различных процессов.

Рассматриваемая политика охватывает весь штат компании. Важно, чтобы она строго исполнялась. Такая политика нацелена на усиление общей политики безопасности компании. Всех сотрудников необходимо уведомить о положениях политики. Они должны «нести ответственность за обеспечение безопасности данных в рамках своих должностных обязанностей» [8].

Требования, которые выдвигаются к обеспечению надлежащей защиты сведений, обозначены в различных документах. Они и представляют собой политику информационной безопасности фирмы. В них также указаны главные ориентиры организации по защите данных. Существует 3 главных уровня формирования такой политики: нижний, верхний, средний.

Благодаря верхнему уровню появляется возможность:

– сформировать собственные нормы, правила, политику безопасности для регулирования тех или иных аспектов;

– уведомить персонал о главных приоритетах и задачах в сфере безопасности данных компании.

На среднем уровне рассматриваемая политика позволяет отразить требования, которые выдвигаются компанией к таким аспектам:

– применению информационных систем;
– способам и технологиям обработки данных;
– субъектам, которые занимаются обработкой сведений. Обеспечение защиты данных в компании находится в прямой зависимости этих людей.

«Нижний уровень изучаемой политики предназначен для анализа тех или иных документов, операций, которые осуществляются с целью обеспечения надлежащей безопасности данных в компании» [40].

Далее следует отметить стадии формирования политики информационной безопасности в компании. К ним относятся:

– оценка того, как владельцы и работники компании относятся к угрозам безопасности;
– изучение значимых информационных активов компании;
– определение угроз безопасности, которые существуют на текущий момент. Осуществление оценки рисков.

При формировании политики информационной безопасности необходимо учитывать, что на нижнем уровне она должна отвечать той политике, которая сформирована на верхнем. Важно, чтобы в соответствующих документах были четко обозначены нормы и правила. Текст политики должен излагаться лаконично и понятным языком для работников компании. Особую важность для защиты сведений в компании имеет политика безопасности, которая представляет собой системы данных. Они тесно взаимосвязаны между собой. Такие структуры применяются для защиты данных на каждом уровне функционирования организации [18].

Гудхью и Штрауб выделили четыре компонента мер безопасности: Сдерживающие контрмеры, как правило, не основаны на технологиях и

направлены на предотвращение инцидентов информационной безопасности. Сдерживающие контрмеры включают в себя политику безопасности и обучение навыкам безопасности. Напротив, «цель превентивных контрмер безопасности состоит в том, чтобы фактически предотвратить возникновение инцидента информационной безопасности с помощью политики информационной безопасности» [42].

Далее, следует изучить главные компоненты политики рассматриваемой безопасности. Благодаря ей специалисты той или иной компании могут проводить аудит защиты сведений – как внутренний, так и внешний. Полученные результаты в дальнейшем применяются с целью определения того, насколько эффективными являются способы защиты.

Необходимо постоянно улучшать и обновлять данную политику. Корректировки, которые были внесены, важно постоянно сравнивать с уже применяемыми средствами защиты.

Рассматривая глобальную политику безопасности компании, можно отметить, что правила дифференцируются на такие категории:

VPN. Такие правила реализуются с помощью специальных протоколов IPSec. Драйвер VPN в данном случае – это агент выполнения правил. Он находится в шлюзах безопасности;

- пакетная фильтрация. Эти правила обеспечивают фильтрацию таких пакетов: stateless, stateful;
- прокси. Правила подразумевают активацию защиты от вирусов и других вредоносных программ. Они обеспечивают фильтрацию трафика, поступающего через прикладные протоколы. В этой ситуации прокси-агент играет роль исполнительного агента;
- авторизованный доступ. Чаще всего подразумевается использование принципа одноразового входа. Такие правила дают возможность обеспечить деятельность пользователей по соответствующим паролям. Их исполняют агенты разных уровней, под которыми подразумеваются системы авторизации;

– правила обеспечения формирования протокола событий. Они также отвечают за протоколирование слабых мест в общей системе защиты данных. Учет событий осуществляет специальный агент. Роль исполнителя играет информационная система в целом.

С помощью локальной политики безопасности предприятия выполняется настройка средств защиты информации и реплицируются настройки для узлов с выполнением их последующей корректировки. В целом «в локальной политике безопасности предприятия размещены правила с помощью, которых регламентируются соединения, меняются настройки используемых сетевых устройств» [11].

В организации при работе с большим объемом конфиденциальных сведений стоит первоочередная задача организации защиты информации, т.е. определения мероприятий, направленных на создание, обеспечение и поддержку информационной безопасности. «Объект защиты информации представляет собой информацию или информационный процесс, который требует обеспечения защиты от несанкционированного доступа, нарушения целостности и структурированности данных» [3].

Цель защиты информации - это получение результатов от предотвращения ущерба, обусловленного утечкой или несанкционированным воздействием на информацию. Эффективность защиты информации позволяет определить уровень соответствия результатов используемой системы защиты данных поставленным целям. Выделяют следующие основные виды защиты информации:

– Защита информации от утечек – это мероприятия, направленные на сохранность и целостность конфиденциальных данных, используемых во внутреннем и внешнем документообороте предприятия.
– Защита данных от разглашений – это мероприятия, направление на предотвращение неосторожных, умышленных действий сотрудников или иных лиц, огласивших конфиденциальную

информацию, что может привести к дальнейшей передаче данных.

– Защита данных от несанкционированного доступа (НСД) – это мероприятия, направленные на запрет доступа к компьютерной сети за счет применения комплекса инженерно-технических, программных и организационных средств.

Кроме того, необходимо разработать систему защиты данных, включающую совокупность технических, программных, криптографических и организационных средств, позволяющих обеспечить безопасность сети в любой момент времени от случайного или преднамеренного воздействия, а также несанкционированного использования.

«Информационная безопасность выступает одной из главных проблем современного общества и обусловлена увеличением значимости информации в основных бизнес-процессах» [41].

Проблемы защиты информации в настоящее время связаны с дестабилизирующим воздействием внешних и внутренних угроз, возникающих в организации и влияющих на ее функционирование. В свою очередь, понятие проблема безопасности данных взаимосвязано с понятием угроза безопасности. Это привело к тому, что в деятельности предприятий все больше возникает проблем, оказывающих негативное влияние на систему управления, а также технологическую поддержку в вопросах хранения и обработки данных. Поэтому методы и инструменты для обеспечения комплексной системы защиты на предприятии должны выполнять мониторинг угроз на уровне информационного, аппаратного и программного обеспечения. Развитие компьютерных технологий, аппаратного и программного обеспечения расширило круг проблем защиты информационных потоков, циркулирующих в компьютерных сетях от несанкционированного доступа. «Основной проблемой является необходимость обеспечения требуемого уровня защиты, при котором необходимо учитывать, что информация, передаваемая по компьютерной сети, может быть получена злоумышленником и передана по каналам связи» [11].

Проблемы информационной безопасности разделяют на три основных вида:

- «перехват данных, связанный с нарушением конфиденциальности информации;
- модификация или изменение данных, связанных с изменением исходного сообщения или полной его подмены с последующей пересылкой адресату;
- нарушение авторства информации, то есть передача информации не от имени автора, а от имени злоумышленника» [23].

Главной целью стандартизации является повышение доверия, выполнение необходимых мероприятий по защите информации от возникающих угроз и внедрение методов для снижения рисков.

Чтобы гарантировать эффективную защиту информации компании, необходимо разрешить целый ряд задач. К ним относятся:

- обеспечить надлежащее качество работы структурных подразделений в сфере безопасности данных компании;
- регулярно вносить изменения в систему защиты сведений;
- формировать планы, направленные на эффективное управление рисками нарушения безопасности данных. Также необходимо обеспечить интеграцию планов в главные бизнес-процессы компании;
- регулярно вносить необходимые изменения во внутренний документооборот в сфере защиты сведений;
- принимать результативные решения в сфере улучшения системы защиты сведений. Также необходимо составлять современные программы обучения персонала;
- выполнять наблюдение за обнаружением угроз, улучшать меры, направленные на их устранение;
- использовать современные способы защиты сведений. Необходимо также регулярно осуществлять внутреннюю и внешнюю проверку

безопасности в сфере информационных технологий;

- принимать результативные решения в сфере улучшения политики безопасности компании. Также необходимо вносить изменения в соответствующие планы и стратегии.

Выше были обозначены главные задачи. Именно они станут базой организации системы безопасности и защиты сведений в данной компании.

1.2 Процессы управления информационной безопасности

Процессы управления информационной безопасности.

Процессы планирования СУИБ.

Формирование политики информационной безопасности.

Цель: задокументировать правила работы в организации в области информационной безопасности политика информационной безопасности – правила, процедуры, практические приемы и руководящие принципы в области информационной безопасности, которыми руководствуется организация в процессе своей деятельности.

Политика информационной безопасности описывает:

- цели деятельности организации;
- приоритет направления обеспечения информационной безопасности может быть определен в политике информационной безопасности в зависимости от направления бизнеса организации;
- структуру управления информационной безопасности;
- построение системы информационной безопасности – определяется, каким образом создается система информационной безопасности, для достижения необходимого уровня информационной безопасности, соответствующего целям информационной безопасности;
- цели по обеспечению, обучению и осведомлению информационной безопасности;

- обеспечение поддержки и проверки информационной безопасности;
- основывается на управлении рисками информационной безопасности. Оценка информационной безопасности производится при проведении внешних и внутренних аудитов и мониторинга;
- политика информационной безопасности указывает на необходимость проверок, их видов и периодичность;
- обстоятельства, при которых политика информационной безопасности должна быть пересмотрена или скорректирована;
- в зависимости от размера и структуры организации, структура управления информационной безопасности включает роли;
- совет по информационной безопасности (комитет) – ответственность за формирование и утверждение политики, проведение мониторинга эффективной политики информационной безопасности, принятие решений по ресурсам (люди, финансы), необходимые для обеспечения информационной безопасности;
- ответственный за политику информационной безопасности - контроль реализации политики, аудит, мониторинг процессов и защитных мер по обеспечению информационной безопасности;
- служба безопасности или администратор – применение и выполнение процессов и процедур по обеспечению информационной безопасности, администрирование средств, реализующих защитные меры, обработка инцидентов информационной безопасности.

В результате можно сделать вывод о том, что приведены мероприятия при разработке политики информационной безопасности.

Установление контекста управления рисками.

Цель: установление внешнего и внутреннего контекста управления рисками, который включает установление критериев, необходимых для управления информационной безопасности, и области применения управления рисками информационной безопасности.

При установлении критериев принятия риска организация учитывает:

- соблюдение договорных обязательств организации;
- финансовые и материальные последствия;
- соблюдение законодательства;
- репутация и доверие к организации со стороны заинтересованных лиц;
- безопасность, здоровье работников организации;
- эффективность и непрерывность бизнес – деятельности.

Организация должна определять область применения управления рисками информационной безопасности для выбранного объекта, при этом область применения должна охватывать все значимые активы выбранной области [9].

Результат: установленная область применения управления рисками информационной безопасности и критерии оценивания рисков, критерии влияния риска и критерии принятия риска.

Оценка рисков информационной безопасности.

Идентификация и определение ценности активов.

Ценность актива включает стоимость актива или затраты по замене поврежденного актива и расходы из-за потери свойств информационной безопасности (конфиденциальности, целостности, доступности).

Ценность актива, в зависимости от характеристик, делится на степени:

- минимальная – устанавливается для активов, утрата которых или потеря свойств безопасности может привести к незначительному снижению качества и снижению доступности;
- средняя – устанавливается для актива, утрата которых или потеря свойств безопасности, может привести: нарушению отдельных договоров обязательств организации и нарушению конфиденциальности информации, связанной с предоставлением услуг;
- высокая – устанавливается для актива, утрата которого или набор

свойств безопасности, может привести к нарушению законодательных требований, снижению репутации и доверия со стороны других организаций и лиц, невыполнению договорных обязательств, нарушению конфиденциальности персональных данных, нарушению непрерывности бизнес – процессов;

– критическая - устанавливается для актива, утрата которого или набор свойств безопасности, может привести к нарушению законодательных требований, невыполнению договорных обязательств организации, потеря репутации и утрата доверия со стороны других организаций и лиц, нарушению конфиденциальности персональных данных и сведений, составляющих конфиденциальную тайну, невозможность осуществления бизнес – процессов.

В определении ценности активов участвуют владельцы активов, служба ИБ, представители руководства организации.

Результат: список активов и их ценностей.

Идентификация угроз.

Цель: идентификация угроз и возможность их реализации.

Информация об угрозах может быть получена от владельцев активов (процессов), собственников систем, в результате анализа инцидентов, из любых нормативных документов, представляющих список возможных угроз [33].

Оценка угроз зависит от степени детализации модели угроз, учитывающей основные признаки угроз. «Оценка признаков и их обобщение позволяет получить оценку опасности любых идентифицированных угроз» [10].

При оценке угроз следует учитывать и оценивать следующие атрибуты угроз:

– продолжительность и непрерывность реализации угрозы информационной безопасности;

– степень локализации угрозы;

– возможность обнаружения угрозы;

– возможность нейтрализации угрозы;

– частота реализации угрозы;

– источник угрозы.

Результат: перечень идентифицированных актуальных угроз для активов и оценка возможности их реализации.

Идентификация уязвимостей.

Цель: определение уязвимостей активов и оценка их уровня.

Данные для идентификации и оценки уязвимостей могут быть получены от владельцев активов, специалистов информатизации и информационной безопасности, поставщиков компонентов системы. Уязвимости необходимо идентифицировать для каждого типа активов и зафиксировать в перечне.

Уровень уязвимостей определяется степенью существования уязвимости в активе и возможностью использования этой уязвимости угрозой.

Для каждого актива должны быть определены уровни всех присущих данному активу уязвимостей и зафиксированных в перечне уязвимостей.

Результат: перечень уязвимостей активов и оценка их уровней.

Идентификация существующих защитных мер.

Цель: определить существующие защитные меры и их эффективность.

Идентификация существующих защитных мер необходима для того, чтобы избежать дублирования защитных мер и лишних расходов. Необходимо провести проверки для того, чтобы убедиться в правильности функционирования и использования защитных мер там, где это необходимо.

Результат: перечень всех существующих защитных мер, их места нахождения и состояния использования.

Идентификация последствий.

Цель: идентификация последствий для активов, в результате потери конфиденциальности, целостности, доступности.

Существует два вида последствий:

– операционные последствия. Потеря времени на ремонт или замену актива; снижение безопасности сотрудников, вследствие нарушения информационной безопасности; финансовые затраты, связанные со стоимостью восстановления или приобретения актива;
– последствия, связанные с потерей бизнеса (деятельности). Потеря репутации, вследствие нарушения законодательных (нормативных) обязательств, или вследствие использования внешней стороной информации, полученной из-за нарушения информационной безопасности.

Последствия определяются с помощью идентификации инцидентов и их сценариев.

Сценарий инцидента – описание угрозы, использующий определенную уязвимость или набор уязвимостей во время инцидента.

Результат: перечень сценариев инцидента с их последствиями.

Оценка последствий.

Цель: оценка влияния инцидентов на бизнес (деятельность) объекта, с учетом последствий нарушения информационной безопасности (конфиденциальности, целостности, доступности).

Для оценки последствий необходимо знать перечень идентифицированных сценариев инцидентов с их последствиями.

Оценка последствий связана с анализом влияния на бизнес (деятельность) на основе определения ценности активов. В каждой последующей интеграции оценки она будет отличаться (снижаться) из-за наличия и степени эффективности реализации защитных мер [36].

Результат: перечень последствий сценариев инцидентов и их оценка.

Оценка вероятностей инцидентов.

Цель: оценка вероятности (возможности) сценариев инцидентов.

Для оценивания вероятности инцидентов необходим перечень идентификационных сценариев инцидентов с их последствиями, перечень существующих защитных мер.

Необходимо учитывать уровни угроз и уровни уязвимостей, а также перечень существующих защитных мер и их эффективность.

Результат: оценка вероятности (возможности) сценариев инцидентов.

Определение уровня риска.

Цель: определение уровня риска для сценариев инцидентов.

Под уровнем риска понимается величина риска, выраженная комбинацией последствий и их вероятностей.

Для определения уровня риска необходим перечень сценариев инцидентов с их последствиями, перечень активов и их оценка, вероятность сценариев инцидентов.

Результат: перечень рисков и значения их уровней.

Оценивание риска.

Цель: сравнение уровней рисков с критериями оценивания риска и критериями принятия риска.

Оценивание риска – это процесс сравнения результатов анализа риска с критериями риска с целью определения, является ли риск и его величина приемлемыми (допустимыми).

Для того чтобы осуществить оценивание риска необходимы: перечень рисков с их значениями; критерии оценивания риска; критерии принятия риска.

При оценивании риска подготавливается информация для принятия риска и дальнейших действий с ним.

Результат: перечень рисков с назначенными приоритетами их обработки, в соответствии с критериями оценивания риска; перечень приемлемых рисков, в соответствии с критерием принятия риска.

Обработка рисков.

Цель: снижение риска до приемлемого уровня и определение плана обработки рисков.

Под обработкой риска понимается процесс модификации риска. Для обработки риска возможны следующие действия:

- сохранение риска – если уровень риска приемлемый и соответствует критериям принятия риска;
- предотвращение риска - осуществляется путем отказа от действий или условий, вызывающих конкретный риск;
- разделение риска – риск разделяется с другой стороной, которая может эффективно снизить риск;
- снижение риска – осуществляется путем введения защитных мер для того, чтобы остаточный риск соответствовал приемлемому уровню.

«При выборе защитных мер должны быть учтены функциональные характеристики защитных мер, а именно: простота, прозрачность для пользователя, стойкость защитных мер, типы выполнения функций (предотвращение, сдерживание, обнаружение, восстановление, мониторинг)» [24].

Результат: решение о выборе защитных мер (план обработки риска) и остаточные риски.

Принятие рисков.

Цель: формирование решений о принятии риска.

Формирование решений принимается руководством организации.

Для принятия рисков необходим план обработки рисков, остаточный риск и их оценка.

Уровень остаточного риска может не соответствовать критериям принятия риска.

Результат: перечень принятых рисков с обоснованием сохранения тех рисков, которые не соответствуют критериям принятия риска.

Формирование политик информационной безопасности автоматизированных систем (АС).

Цель: формирование политик автоматизированных систем (далее - АС) с учетом политики информационной безопасности и результатов управления рисками.

Политика информационной безопасности АС должна содержать:

– описание системы, ее компонентов и определение ее границ, а также описание целей с точки зрения бизнеса;
– описание целей информационной безопасности системы;
– описание (перечень) активов системы;
– описание угроз, снижение защищенной актуальности для системы;
– описание уязвимостей системы и ее компонентов;
– описание рисков информационной безопасности системы;
– перечень защитных мер.

В результате, указанные меры входят в состав политики информационной безопасности.

Процессы реализации и эксплуатации системы управления информационной безопасности

Реализация защитных мер. Цель: реализация защитных мер.

Перед реализацией защитных мер должны быть протестированы. По результатам тестирования составляется отчет.

Для дальнейшего использования и эксплуатации защитных мер разрабатываются должностные инструкции по эксплуатации защитных мер и регламенты использования защитных мер.

Результат: реализованные защитных мер.

Управление изменениями автоматизированных систем. Цель: контроль соответствия изменений АС требованиям информационной безопасности. Управление изменениями АС заключается в следующем:

– идентификация и регистрация изменений АС. При этом должно быть точно установлено, что все действия по предъявлению и рассмотрению этих изменений, а также внесение изменений производится уполномоченными лицами;
– анализ и оценка влияния последствий на информационной безопасности;
– учет количества изменений и хронология;
– обновление и корректирующие документации по АС после

завершения каждого изменения. Старая документация архивируется, либо уничтожается;

- реализация изменений должна производиться таким образом, чтобы не нарушать реализацию процессов;
- сообщение уполномоченным лицам об изменениях.

Результат: учет всех принятых изменений АС.

Реализация программы осведомления об информационной безопасности.

Цель: увеличить уровень осведомления об информационной безопасности таким образом, чтобы информационная безопасность стала неотъемлемой частью деловой деятельности сотрудников.

Управление инцидентами информационной безопасности.

Цель: реагирование на инцидент рациональным и эффективным способом; получение знания и опыта из инцидента для использования его в будущем.

Для управления инцидента информационной безопасности должны быть регламентированы следующие процедуры:

- обнаружение и оповещение об инциденте информационной безопасности. Осуществляется сотрудниками и (или) техническими средствами на основе признаков инцидента. Сотрудник, путем наблюдения или с помощью АС, должен сформировать отчет об инциденте информационной безопасности;
- анализ инцидентов ИБ. Заключается в сборе информации об инциденте и принятии решения о реализации инцидента или личности инцидента;
- сдерживание инцидентов информационной безопасности. Заключается в выборе стратегии сдерживания. В организации должна быть определена стратегия для каждого типа инцидента;
- устранение инцидентов информационной безопасности и восстановление после них. Заключается в устранении элементов

инцидента после сдерживания;

- сбор и обработка данных об инцидентах информационной безопасности и подготовка отчета об инциденте информационной безопасности. Заключается в сборе данных, которые могут быть использованы при обработке инцидента, статистических данных об инциденте и создании хронологии событий.

Результат: управление инцидентами рациональным и эффективным способом.

Мониторинг информационной безопасности.

Целями мониторинга информационной безопасности являются:

- контроль за реализацией в организации положений внутренних и внешних документов по информационной безопасности для обнаружения отклонений от требований информационной безопасности;
- контроль качества используемых защитных мер;
- выявление нештатных, в том числе злоумышленных действий с информационными активами и бизнес-процессами организации;
- выявление событий информационной безопасности, часть из которых в дальнейшем классифицируется как инциденты информационной безопасности;
- выявление уязвимостей активов, которыми могут воспользоваться злоумышленники для реализации атак на системы, сети и сервисы организации;
- обеспечение доказательной базы для расследования инцидентов.

Процессы мониторинга информационной безопасности включают в себя следующую деятельность:

- поиск, отслеживание, наблюдение, накопление, систематизация, оценивание сведений, относящихся к области информационной безопасности;
- прогнозирование состояния и качества всех объектов и процессов в

информационной среде организации.

Для реализации мониторинга информационной безопасности необходимо создавать журналы для записей событий, связанных с информационной безопасности. Записи мониторинга информационной безопасности следует хранить в течение установленного времени, с целью использования при расследовании инцидентов информационной безопасности, а также с целью корректирующих защитных мер [29].

При реализации мониторинга фиксируют, как правило, следующие параметры событий: дата/время входа в систему; идентификатор терминала; успешные (не успешные) попытки доступа в систему. «Мониторинг реализуется для таких событий, как авторизованные действия, привилегированные действия и другие» [5].

Результат: данные журналов регистрации событий.

Проверка соответствия информационной безопасности. Цели проверки соответствия информационной безопасности:

- поиск и контроль несоответствия установленных требований информационной безопасности;
- поддержка информативности руководства об информационной безопасности.

Способы проверки соответствия информационной безопасности:

- самооценка информационной безопасности;
- внешний и внутренний аудит информационной безопасности.

Самооценка информационной безопасности – самостоятельный, документированный процесс оценки свидетельств самооценки с целью установленной степени выполнения требований по обеспечению информационной безопасности.

Свидетельства самооценки информационной безопасности – записи, изложения фактов или другая информация, которые имеют отношение к требованиям информационной безопасности и могут быть проверены.

Самооценка информационной безопасности проводится по инициативе руководства организации и, как правило, собственными силами. Цели самооценки зависят от руководства организации.

Результат: отчет по самооценке информационной безопасности.

«Аудит информационной безопасности – периодически независимый и документированный процесс, получение свидетельства аудита информационной безопасности и объективов их оценивания, с целью установленной степени выполнения согласованных критериев аудита информационной безопасности» [16].

Свидетельства аудита информационной безопасности – записи, изложения фактов или другая информация, которые имеют отношение к требованиям информационной безопасности и могут быть проверены.

Внутренний аудит информационной безопасности проводит для своих целей сама организация.

Внешний аудит проводит стороны, заинтересованные в деятельности организации.

Результат: отчет и заключение по результатам аудита информационной безопасности.

Анализ информационной безопасности со стороны руководства.

Цель: обеспечить уверенность в том, что система управления информационной безопасности является адекватной ее назначению; определение возможности улучшений процессов управления информационной безопасности.

Анализ информационной безопасности позволяет оценить, нужны ли улучшения и изменения в отношения информационной безопасности. Для процесса анализа необходимо определить необходимый набор данных, которые должны содержать следующую информацию:

- результаты аудитов и самооценки информационной безопасности;
- результаты мониторинга информационной безопасности;
- способы, методы и процессы, которые могут использоваться в

организации для улучшения функционирования защитных мер и эффективности системы управления информационной безопасности;

- уязвимости и угрозы, которые не были рассмотрены при оценивании риска;
- действия, предпринятые по итогам предыдущего анализа информационной безопасности со стороны руководства.

Результат: документы, в которых представляются рекомендации и предложения по улучшению информационной безопасности.

Процессы совершенствования СУИБ.

Цель: реализация принятых решений по улучшению системы управления информационной безопасности.

К процессу совершенствования информационной безопасности относятся: «реализация улучшений в информационной безопасности; информирование об изменениях и их согласования с заинтересованной стороной» [19].

Совершенствование СУИБ осуществляется путем использования политики информационной безопасности, целей организации, результатов аудитов внутренних и внешних, анализа отслеживаемых событий, корректирующих и превентивных мер и анализа со стороны руководства.

Реализация корректирующих действий в отношении защитных мер осуществляется для установки причины несогласования защитных мер или других нежелательных ситуаций, приводивших к снижению уровня информационной безопасности, чтобы предотвратить их повторения. Процедура действий в отношении защитных мер АС должны предпринимать для устранения причин возможной несогласованной защитных мер или других возможностей нежелательной ситуации.

На основании реализации корректирующих действий в отношении защитных мер осуществляется информирование и согласование с заинтересованными сторонами о внесенных улучшениях.

Результат: корректирующие действия в отношении системы управления информационной безопасности и плана обработки рисков.

Итак, в результате исследования можно сделать вывод о том, что мероприятия должны реализоваться в систему (циклическую) для обеспечения конфиденциальности информации и связанных с ней процессов (обработки исходных данных).

Преимущества, системы управления информационной безопасности заключаются в том, что предполагает планирование и практическая реализация процессов по обеспечению информационной безопасности направлены на минимизацию рисков и контроль.

1.3 Контроль и методы обеспечения информационной безопасности

Существуют стандарты безопасности данных, которые приняты на международном уровне. К примеру, ISO 17799 под названием «Нормы при обеспечении безопасности данных». Такие стандарты включают в себя описание общих рекомендаций, направленных на обеспечение надлежащего уровня безопасности сведений. В упомянутом выше стандарте подробно обозначены правила, которые важно принимать во внимание в процессе формирования политики безопасности данных. Также их следует учитывать во время проектирования тех или иных мероприятий, нацеленных на защиту сведений [4].

Рассматриваемый международный стандарт включает в себя несколько разделов. Они устанавливают ряд векторов в сфере обеспечения безопасности информационных систем. К ним относятся:

- политика такой безопасности указывает на необходимость поддержки со стороны руководителей компании системы организации безопасности информационных сведений;
- представлены рекомендации касательно рассматриваемой политики компании. Они обозначены в главе «Вопросы организационного

характера»;

- мероприятия, направленные на обеспечение надлежащего уровня безопасности сведений. Они указаны в главе «Классификация информационных данных»;
- влияние человека, правила, которые созданы с целью минимизации риска безопасности. Данные нормы указаны в главе «Управление кадрами»;
- обеспечение безопасности физического типа определяет действия, которые направлены на обеспечение безопасности элементов системы данных;
- подробно рассмотрено понятие обеспечения непрерывности бизнес-процессов;
- обозначены основные требования, которые выдвигаются к политике безопасности данных.

Все работники компании, которые осуществляют операции с информацией, должны быть в обязательном порядке уведомлены обо всех положениях рассматриваемой политики. Донести их следует в лаконичном и понятном виде.

Важно, чтобы политика безопасности сведений выступала неотъемлемым компонентом общей политики компании, которая отражена в соответствующих документах. Если политика безопасности информационных данных действует и за пределами фирмы, необходимо приложить усилия для предупреждения распространения сведений конфиденциального характера [13].

Благодаря классификации угроз появляется возможность находить угрозы в соответствующих категориях. Они подлежат оценке и анализу, после чего формируется стратегия предупреждения или ослабления их влияния на общую систему.

Эксперты сформулировали несколько определений, которые раскрывают термин «информационная безопасность». В качестве примера

можно привести следующее определение: сохранение доступности, целостности и конфиденциального характера сведений.

На протяжении последних 5-ти лет все чаще стали наблюдаться такие атаки:

– использование уязвимостей;

– использование компьютерных вирусов;

– получение конфиденциальных данных мошенническим путем (фишинг);

– DOS и DDOS;

– социальная инженерия.

По мере того, как современные атаки становятся все более совершенными, меры защиты от DDoS-атак помогают обеспечить безопасность [43].

Необходимо отметить, что социальная инженерия является одной из актуальных угроз.

В компьютерной безопасности уязвимость — это «слабость, которая позволяет злоумышленнику снизить уровень безопасности системы» [44].

Уязвимость - это пересечение трех элементов: восприимчивость или недостаток системы, доступ злоумышленника к недостатку и способность злоумышленника использовать недостатки.

Чтобы использовать уязвимость, злоумышленник должен иметь хотя бы один применимый инструмент или метод, которые могут подключаться к слабости системы.

Управление уязвимостями — это циклическая практика выявления, классификации, исправления и смягчения уязвимостей. Эта практика обычно относится к уязвимостям программного обеспечения в вычислительных системах [16].

Использование уязвимости с тем же значением риска может привести к путанице. Риск связан с потенциалом значительной потери. Тогда есть уязвимости без риска: например, когда затронутый актив не имеет значения.

Уязвимость, связанная с одним или несколькими известными случаями работающих и полностью реализованных атак, классифицируется как уязвимость, которую можно использовать, — уязвимость, для которой существует эксплойт.

«Ошибка безопасности (дефект безопасности) является более узкой концепцией: есть уязвимости, которые не связаны с программным обеспечением: уязвимости, связанные с оборудованием, сайтом, персоналом, являются уязвимостями, которые не являются ошибками безопасности программного обеспечения» [45].

Выбор правильных элементов управления и их реализация первоначально помогут организации снизить риск информационной безопасности до приемлемых уровней. Выбор контроля должен следовать и должен основываться на оценке риска.

Элементы управления могут различаться по своему характеру, но в принципе они являются способами защиты конфиденциальности, целостности или доступности информации. ISO / IEC 27001: 2005 определил 133 элемента управления в разных областях, но это не является исчерпывающим.

Организации могут осуществлять дополнительные меры контроля в соответствии с требованиями организации.

«Административный контроль (также называемый процедурным контролем) состоит из утвержденных письменных политик, процедур, стандартов и руководящих принципов» [22].

Административный контроль формирует рамки для ведения бизнеса и управления людьми. Они информируют людей о том, как вести бизнес и как проводить ежедневные операции. В некоторых отраслях промышленности есть политики, процедуры, стандарты и руководящие принципы, которым необходимо следовать — такой пример -стандарт безопасности данных платежных карт (PCI DSS), требуемый Visa и MasterCard [38].

Другие примеры административного контроля включают политику безопасности, политику паролей, политику найма и дисциплинарные меры.

Административный контроль служит основой для выбора и реализации логического и физического контроля. Логические и физические элементы управления - это проявления административного контроля. Административный контроль имеет первостепенное значение.

Логические средства управления (также называемые техническими средствами управления) используют ПО и данные для мониторинга и контроля доступа к информационным и вычислительным системам. Например: пароли, сетевые и межсетевые экраны на основе хоста, сетевые системы обнаружения вторжений, списки управления доступом и шифрование данных - это логические элементы управления.

Важным логическим управлением, которое часто упускается из виду, является принцип наименьших привилегий. Принцип наименьших привилегий требует, чтобы индивидуальный, программный или системный процесс не предоставлял больше прав доступа, чем это необходимо для выполнения задачи.

Доступ к защищенной информации должен быть ограничен лицами, имеющими право доступа к информации. Также должны быть разрешены компьютерные программы, и во многих случаях компьютеры, которые обрабатывают информацию [11].

Эффективная защита обеспечивается инструментами контроля доступа к охраняемым данным. Необходимо постоянно улучшать такие инструменты. Чем большую ценность имеют сведения, тем более мощными должны быть инструменты контроля доступа к ним. Они формируются на базе аутентификации и идентификации.

Существует 3 стадии контроля доступа. К ним относятся: авторизация, аутентификация, идентификация.

Авторизация доступа к сведениям начинается с операций административного характера. Административная политика регламентирует, какие люди и при каких обстоятельствах могут получить этот доступ.

Инструменты контроля доступа ориентированы на обеспечение строгого соблюдения административных политик. Система предлагает такой механизм управления доступом, который базируется на одном из перечисленных выше методов. Иногда сочетаются все три способа.

Способы обеспечения безопасности сведений включают в себя такие аспекты: правовые, организационно-технические, экономические.

Организационно-технические способы охватывают:

– систему обеспечения информационной безопасности. Речь идет о мероприятиях и технических средствах. К мероприятиям относятся правила работы со сведениями, к техническим средствам – применение специальных устройств и программ для сохранения конфиденциального характера сведений;

– формирование, использование, улучшение методов защиты сведений, которые применяются на данный момент;

– постоянный контроль над эффективностью мер, которые принимаются в сфере обеспечения информационной безопасности.

Такой контроль имеет огромное значение. Результативность информационной безопасности можно правильно определить только с использованием методики оценки. Если показатели эффективности снижаются, важно как можно скорее внести изменения. Именно поэтому контроль должен быть постоянным.

Рассматриваемые методы тесно коррелируют с правовыми способами информационной безопасности России.

Правовой аспект безопасности России включает в себя следующее:

– выдачу лицензий на выполнение деятельности в сфере обеспечения информационной безопасности;

– прохождение процедуры сертификации технических средств защиты сведений;

– прохождение процедуры аттестации объектов информатизации. Аттестация проводится согласно положениям информационной безопасности России.

Экономический компонент подразумевает:

– разработку программ, направленных на обеспечение безопасности сведений в России;

– выбор источников финансирования таких программ;

– формирование порядка обеспечения финансами данных программ;

– формирование системы страхования рисков информационного типа.

«Под информационной безопасностью подразумевается комплексная структура. Ее главной задачей выступает предупреждение утечки данных конфиденциального характера по техническим путям. Также важнейшей задачей является предотвращение доступа к носителям данных со стороны третьих лиц. В результате обеспечивается целостность информации при взаимодействии с ней. Например, при хранении, обработке и осуществлении других операций. При правильной организации технические меры дают возможность определить применение различных устройств. Они обычно используются для противоправного завладения сведениями» [14].

В РФ существует несколько нормативных правовых документов, регламентирующих работу в информационной сфере: «Об утверждении Доктрины информационной безопасности РФ», «Об информации, информационных технологиях и о защите информации» и т. д. Одним из фундаментальных является Федеральный закон РФ «О коммерческой тайне». К этому перечню стоит добавить Постановления Правительства РФ «О сертификации средств защиты информации», «О лицензировании деятельности по технической защите конфиденциальной информации», а также Приказ ФСБ «Об утверждении Положения о разработке, производстве, реализации и эксплуатации шифровальных (криптографических) средств защиты информации» [16].

Наконец, организационный способ включает в себя такие компоненты:

– формирование режима защиты сведений;

– создание правил отношений между работниками компании;

– определение порядка работы с документацией;

– правила применения технических средств в соответствии с законодательством страны;

– оценка угроз информационной безопасности.

Доступ работников к носителям информации четко регламентирован. Этим обеспечивается защита сведений от несанкционированного доступа. Организационный способ не включает в себя применение технических средств.

Технический способ обеспечения сведений включает в себя использование соответствующего технического инструментария и программ. В качестве примера можно привести прикладное программное обеспечение, системы DLP и SIEM и пр. Благодаря рассматриваемым средствам и программам минимизируется риск утечки сведений через компьютерные устройства [27].

На основе сказанного можно сделать вывод, что обеспечение безопасности сведений выступает комплексной и многоаспектной структурой. Это можно объяснить тем, что информационная система представляет собой многоуровневую структуру. Она включает в себя целый ряд элементов: инструкции; программное обеспечение; сотрудники; технические устройства и пр.

Важно применять различные меры для обеспечения надлежащего уровня безопасности данных. К ним относятся: организационные, правовые, технические. Следует применять все указанные меры комплексно, в противном случае появляется риск утери, разглашения данных. В современном социуме информация имеет огромное значение, а особенно актуальная, поэтому ее нужно надежно защищать.

1.4 Методы выявления актуальных угроз информационной безопасности

Анализ материалов доступных источников показывает, что в настоящее время известно большое количество сетевых атак, которые осуществляется с целью нарушения конфиденциальности, целостности и доступности информационных ресурсов в зависимости от возможностей злоумышленников по доступу к ресурсам локальных вычислительных сетей, уровню компетенции, оснащенности и уровня мотивации нарушителей, ущерб может быть различен. Проведенные исследования экспертно-аналитическим центром InfoWatch в 2020 году свидетельствуют о том, что на протяжении последних лет руководители больше обеспокоены угрозами, исходящими от действий собственных сотрудников подробнее (рисунок 1) [38].

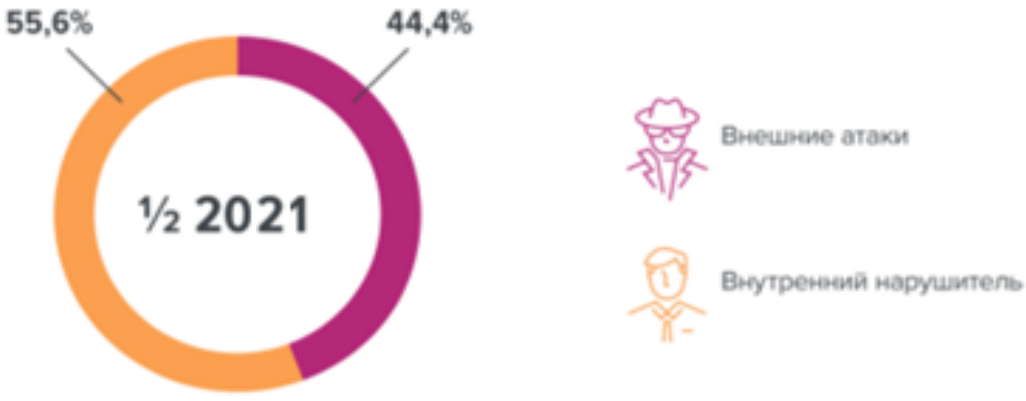

Рисунок 1 – Соотношение опасности внутренних и внешних угроз

Общая характеристика инсайдеров представлена в таблице 1.

Целью выявления угроз информационной безопасности является определение возможности нарушения основных свойств информации в процессе работы.

Таблица 1 – Характеристика типов инсайдеров (подход Фонда InfoWatch)

Тип инсайдеров	Особенности поведения	Опыт работы в сфере информационных технологий	Мотивация	
			Умысел	Корысть
Халатные	Невнимательные, неосторожные	Низкий	Нет	Нет
Манипули-руемые	Ставшие жертвами мошенничества	Низкий	Нет	Нет
Обиженные (саботажники)	Собирающиеся продолжать работу, но считающие, что их деятельность не была по достоинству оценена (низкая зарплата, невысокая должность, отсутствие поощрений и .т.д.)	Средний	Да	Нет
Нелояльные	Собирающиеся увольняться с работы и осуществляющие сбор любой информации на всякий случай	Средний	Да	Нет
Подрабаты-вающие	Решившие дополнительно заработать, или ставшие жертвами шантажа	Средний	Да	Да
Внедренные	Устраивающиеся на работу в подразделения по защите информации с хорошими рекомендациями, работающие до момента получения прав доступа к информационным ресурсам	Высокий, могут использовать средства взлома системы защиты информации	Да	Да

Процесс выявления и определения угроз информационной безопасности должен нести регулярный и систематический характер, и должен осуществляться не только на этапе создания системы информационной безопасности, но и на этапе эксплуатации.

Необходимо наладить процесс своевременного выявления и нейтрализации угроз информационной безопасности, который мог бы предотвратить возможный ущерб.

Экспертный метод.

Оценка возможных угроз безопасности проводится путем формирования экспертной группы, которая проводит анализ уязвимостей. Благодаря качественному формированию экспертной группы можно снизить уровень субъективности при оценке угроз. Состав экспертной группы формируется в соответствии с поставленными вопросами в области информационной безопасности и не может быть меньше количества трех человек. Также этот метод характерен низкими материальными затратами, поскольку задействованные эксперты являются сотрудниками службы. Несмотря на достоинства данного метода, к этому методу можно отнести также ряд существенных недостатков. В первую очередь, это человеческий фактор, который подразумевает определенный уровень субъективности, что может привести к завышению или занижению экспертами прогнозов и предположений в процессе определения угроз информационной безопасности [28]. Стоит отметить, что состав экспертной группы не могут составлять сотрудники, находящиеся на прямом подчинении, поскольку это может увеличить вероятность зависимой оценки. Также, эксперты не должны иметь личный, коммерческий или другой интерес в принятии решения, что также является сложной задачей для определения.

Систематический метод.

Систематический метод выявления угроз информационной безопасности предполагает непрерывный процесс, направленный на выявление и определение угроз, последующую идентификацию источника угрозы и оценку возможного ущерба в случае реализации угрозы. На регулярной основе проводится обзор и переоценка угроз информационной безопасности.

Обеспечение автоматизированного мониторинга может осуществляться руководством предприятия, так и администратором безопасности. Мониторинг и контроль действий персонала также относится к систематическому методу выявление угроз.

Попытка несанкционированного доступа сотрудника того или иного

уровня к конфиденциальной информации будет зафиксирована в системе информационного ресурса, после чего последует процесс идентификации данного нарушения.

В процессе эксплуатации информационной системы соответствующий сотрудник имеет возможность менять ее базовую конфигурацию таким образом, чтобы обеспечить изменение приоритетов значимости обрабатываемой информации в соответствии с появлением новых угроз или новых требований на законодательном уровне.

Необходимость переоценки угроз информационной безопасности также появляется в случаях изменения состава основных компонентов информационной системы, которые могли спровоцировать появление новых уязвимостей, новые сведения о возможных нарушителей и выявление уязвимостей [7].

Метод идентификации возможных источников угроз.

Процесс определения угроз информационной безопасности предполагает систематическую идентификацию источников угроз, оценка возможности и, исходя из этого, выявление актуальных угроз информационной безопасности. Для осуществления идентификации угроз информационной безопасности в информационной системе необходимо выявить следующие критерии:

- способы реализации угроз;
- объекты воздействия, на которые направлена угроза;
- последствия реализации угроз информационной безопасности.

Выявленная таким образом угроза информационной безопасности подлежит нейтрализации.

Правовые методы.

Правовые методы, как правило, направлены на устранение угроз антропогенного характера. В случае нарушения интересов предприятия правовые методы позволяют реализовать механизмы применения определенных санкций в отношение нарушителя. К основным правовым

методам относятся:

- установление порядка защиты и использования информации;
- определение области права обладания информацией;
- сохранение конфиденциальной информации;
- введение мер воздействия за противоправные действия в области использования информационных ресурсов;
- установление права судебной защиты интересов собственника.

Правовые методы противодействия угрозам информационной безопасности реализуются в ходе модернизации нормативно-правовой базы и обеспечивают информационную безопасность, а также способствуют формированию структуры управления.

Экономические методы.

Экономические методы направлены на упразднение источников угроз антропогенного характера, а также на введение в действие механизмов устранения негативных последствий реализации угроз. К экономическим методам можно отнести:

- страхование средств обработки информации;
- страхование информационных рисков;
- введение системы надбавок и коэффициентов;
- введение механизма компенсации ущерба.

Таким образом, проанализированные методы выявления угроз информационной безопасности являются актуальными и основными в процессе обеспечения информационной безопасности предприятия. Данные методы имеют ряд достоинств и недостатков, и нуждаются в дальнейшем усовершенствовании для более эффективного обеспечения информационной безопасности предприятия.

В результате можно сформулировать определенные выводы:

Управление информационной безопасностью - это циклический процесс, включающий осознание степени необходимости защиты

информации и постановку задач; сбор и анализ данных о состоянии информационной безопасности в организации; оценку информационных рисков; планирование мер по обработке рисков; реализацию и внедрение соответствующих механизмов контроля, распределение ролей и ответственности, обучение и мотивацию персонала, оперативную работу по осуществлению защитных мероприятий; мониторинг функционирования механизмов контроля, оценку их эффективности и соответствующие корректирующие воздействия.

На данный момент наблюдается огромное количество угроз для информационных ресурсов той или иной компании. Они делятся на две категории: внешние, внутренние. Оба типа угроз несут серьезную опасность для сведений предприятия.

Поэтому важно обеспечить надлежащий уровень ее защиты.

Необходимость улучшения методов защиты сведений становится все более актуальной по мере внедрения процессов автоматизации. На сегодняшний день информация на бумажных носителях утрачивает свою актуальность и переводится в электронный формат.

Политика в обеспечении информационной безопасности распространяется на всех работников. Политика ИБ, является основой для разработки методик защиты информации в процессе построения системы информационной безопасности.

Необходимо, чтобы система защиты сведений охватывала совокупность средств контроля информационных потоков, наблюдения за локальными сетями и данными, которые компания получает из глобальных сетей и пр. На базе теоретических сведений появляется возможность сформировать информационную безопасность в компании.

Глава 2 Разработка и внедрение комплекса мер по защите информации ООО «Товаротранспортная компания»

2.1 Анализ защиты данных в ООО «Товаротранспортная компания»

Необходимо отметить, что меры по защите информации входят в систему обеспечения информационной безопасности. В свою очередь данные мероприятия входят в организационно-технический метод обеспечения безопасности.

Информационная инфраструктура предприятия представлена следующими подсистемами:

– Сетевая инфраструктура. Для 192 сети выход в Интернет осуществляется посредством использование сетевого шлюза, в качестве которого выступает межсетевой экран D-Link DFL-870 (рисунок 2).

Рисунок 2 – Межсетевой экран D-Link DFL-870

– Межсетевой экран D-Link DFL-870 представляет собой сложное устройство контроля и защиты интернет-соединений, имеющее собственную операционную систему NetDefendOS, список функций которой различен, в зависимости от поставляемой версии.

Основные возможности устройства:

– тип оборудования: активное управляемое (способ управления: Telnet,

веб-интерфейс);

– количество Lan портов: 6, максимальная доступная скорость 4 Гбит/с (доступно автосогласование);

– количество одновременных сеансов: 500 000;

– доступные соединения: PPTP/L2TP/PPPoE, Lan;

– стандарты шифрования: SSL, DES, GRE, IPSEC, IKE/IKEv2;

– технологии межсетевого экрана: NAT, PAT, Zone Defence, TLS (1.0), MAD, RADIUS, LDAP, маршрутизация на основе политик;

–балансировка: перенаправление трафика, балансировка нагрузки сервера;

–антивирусная защита: встроенный сканер (использует сигнатуры серверов Kaspersky), сканирование нешифрованных данных HTTP, FTP, SMTP, POP3, IMAP, сканирование VPN, сканирование передаваемых архивов (ZIP и GZIP);

–фильтрация: белый список, фильтрация поисковых запросов, фильтрация скриптов (Java, JavaScript, ActiveX);

–IDP (система обнаружения вторжений): ведение черного списка IP, обнаружение SMTP вторжений, защита от атак DoS, DDoS, ведение логов;

–управление приложениями: блокировка (распознавание действий свыше 1000 приложений), расписание, контроль ширины пропускания для выбранных приложений.

Веб-интерфейс межсетевого экрана DFL-870 (рисунок 3) имеет классическую систему компоновки – верхнее меню, левое меню, рабочая область настроек справа.

Основные возможности, предоставляемые веб-интерфейсом:

– отображение статистики;

– просмотр журналов (системный журнал, антивирусный журнал, журнал событий приложений, журнал системы обнаружения вторжений, журнал контент-фильтра);

– настройки аутентификации;

– работа с черным списком;

– установка соединений;

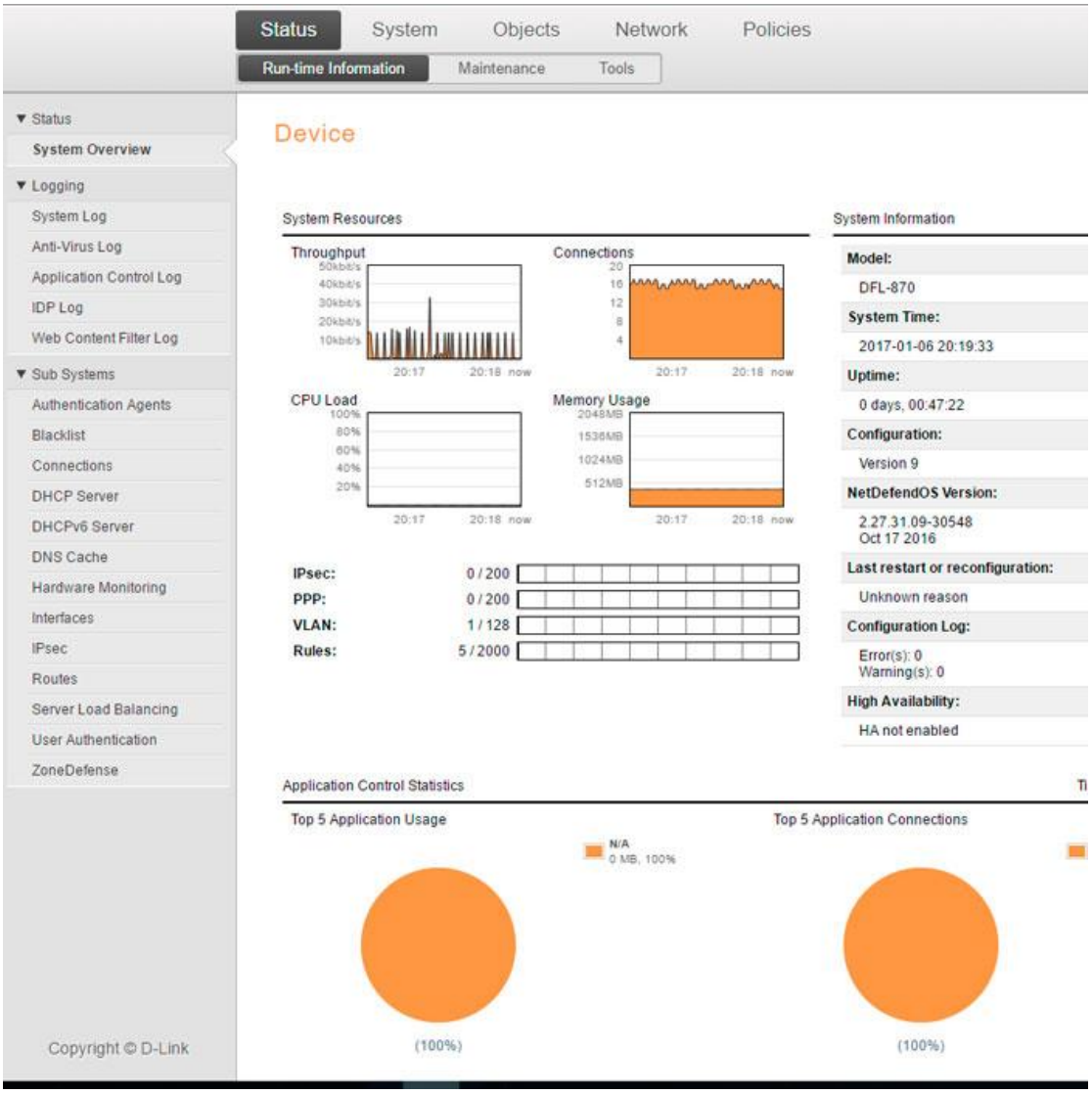

Рисунок 3 – Веб-интерфейс сетевого шлюза D-Link DFL-870

– настройки DCHP (версии 4 и 6);

– управление кешем DNS;

– монитор аппаратных ресурсов;

– управление интерфейсами;

– настройки шифрования IPSec;

– управление маршрутами (включая проброс портов);

– балансировка нагрузки;

– пользовательская идентификация;

– настройка системы ZoneDefence.

Активное сетевое оборудование представлено неуправляемыми коммутаторами D-Link DES-1005D/E, представляющее надежное оборудование для быстрого развертывания локальной сети в рамках офиса (рисунок 4).

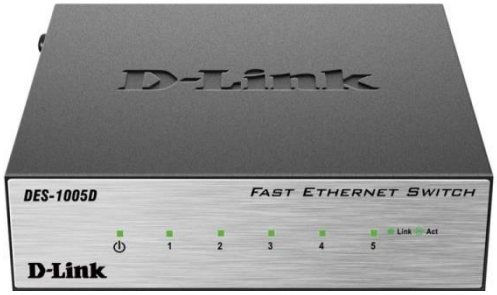

Рисунок 4 – Коммутатор D-Link DES-1005D/E

Коммутатор D-Link DES-1005D/E имеет следующее основные характеристики:

– количество портов: 5 (200 МБ/с);

– Ethernet/Fast Ethernet: полный дуплекс/полудуплекс;

– буфер: 384 Кб на порт.

Данные коммутаторы обладают высокой надежностью и имеют несколько модификаций (большинство из них направлено на поддержку передачи информации посредством различных дополнительных стандартов и протоколов).

Структурная кабельная сеть сформирована по топологии «Звезда», большинство кабинетов имеет собственные коммутаторы D-Link DES 1005D/E из-за ограниченного числа доступных портов в них.

Все компьютеры подключены к единой сети и имеют выход в интернет, на каждом установлен статический IP. На каждом компьютере стоит как

учётная запись пользователя, так и имеется учётная запись администратора для системных настроек.

Дополнительно используются:

– файловый сервер dell;

– сетевые серверы microtik и fujitsu обеспечения непрерывной работы информационных систем 1С и БАРС.

Общая структура сети ООО «Товаротранспортная компания» (рисунок 5).

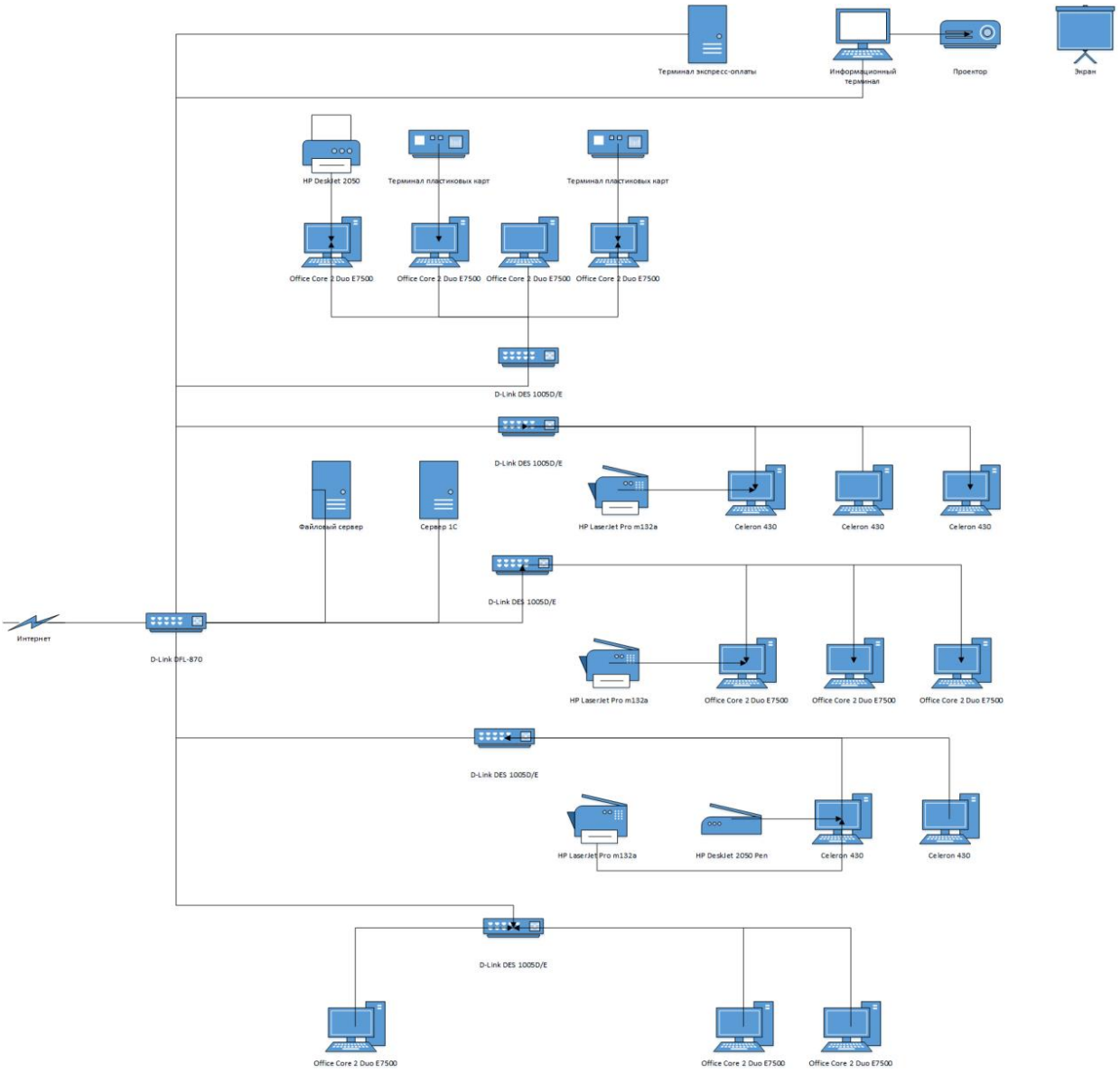

Рисунок 5 – Структура сети ООО «Товаротранспортная компания»

Информационная инфраструктура содержит группировку компьютеров по подразделениям. Ключевые элементы инфраструктуры:

– сетевой шлюз;

– серверы;

– коммутационное оборудование.

Несмотря на то, что серверы не осуществляют поддержку функционирования сетевых соединений, работа подразделений невозможна без их использования, так как на них расположены информационные системы предприятия.

Отдельно следует подключение большого количества сетевых принтеров (в каждом подразделении), что позволяет управлять печатью, выполнять ее резервирование и планирование.

Прочее оборудование, подключенное к автоматизированным рабочим местам сотрудников, не имеет прямого доступа к сети предприятия, либо выполняют соединения самостоятельно (терминалы для оплаты), либо не требуют использования сети.

Автоматизированные рабочие места сотрудников.

Аппаратный комплекс включает в себя устройства - компактные системные блоки Dell Wyse, в которых установлены процессоры Intel(R) Celeron(R) CPU N3060 с частотой 1.6GHz, оперативная память 4Gb, видеокарты Intel(R) HD Graphics под управлением операционной системы Microsoft Windows 10 Pro. 20 рабочих мест представляют собой автоматизированные места NUC, 30 рабочих мест CRAFTWAY. Используются мониторы следующих производителей ViewSonic, Acer, Philips, Dell. Все рабочие места оснащены сетевыми принтерами EPSON WF-M5299 Series, HP LaserJet Pro M203dn, Xerox B210. На каждого пользователя имеется стационарный телефон.

Системы криптографической защиты информации. Так как организация в своей работе использует информационные системы, защита информации основана на использовании средств криптографической защиты. Для

верификации пользователей и данных используются электронные подписи совместно с системой КриптоПро.

КриптоПро представляет собой комплекс криптопровайдеров, выполняющих следующие основные функции:

– генерация ЭП;

– верификация ЭП;

– обслуживание контейнеров ЭП и сертификатов;

– поддержка инфраструктуры открытых ключей;

– сервисные функции (настройка считывателей, перенос сертификатов и закрытых ключей, управление лицензиями и т. д.).

Полный набор утилит КриптоПро позволяет организовать полноценную работу по защите данных:

– при работе в государственных информационных системах посредством использования специального плагина КриптоПро ЭЦП Browser plug-in, устанавливаемый в пользовательский браузер;

– при работе с электронными ключами использованием КриптоПроCSP;

– при организации электронного документооборота за счет использования утилит CriptoProPDF и КриптоПро Office Signature;

– при шифровании файлов любого формата посредством КриптоАРМ.

На аттестованных рабочих местах используется средство мониторинга, обнаружения и предотвращения вторжений Secret Net Studio. Secret Net Studio представляет собой программный комплекс работающий на основе специальных шаблонов настроек в соответствии с выбранным типом автоматизированного рабочего места, необходимого класса защиты и соответствия требованиям ФСТЭК и ФСБ.

Основные функции Secret Net Studio:

– защита от вирусных атак и установки нежелательного программного обеспечения;

– контроль сетевых соединений;

– мониторинг и журналирование инцидентов информационной безопасности автоматизированного рабочего места;

– защита информации от несанкционированного доступа;

– защита объектов программной инфраструктуры автоматизированного рабочего места.

Secret Net Studio обладает широкими возможностями идентификации и разграничения доступа с поддержкой внешних аппаратных ключей доступа к автоматизированному рабочему месту, информационной системе и настройкам операционной системы.

Основной недостаток данного средства выражается в повышенных требованиях к используемым аппаратным ресурсам.

Для доступа к автоматизированным рабочим местам также дополнительно используется (не на всех компьютерах) средство защиты от несанкционированного доступа Dallas Lock, представляющее гибкий программно-аппаратный комплекс. Для управления доступом может использоваться широкий спектр оборудования и способов авторизации:

–закрытый электронный ключ, расположенный на флеш-носителе (доступ по USB);

Система позволяет:

– контролировать доступ к управлению компьютером;

–доступ к отдельным файлам и папкам файловой системы (поддерживается FAT32 и NTFS);

– проводить генерацию паролей различного уровня сложности;

– вести журнал инцидентов информационной безопасности;

– осуществлять контроль целостности аппаратных ресурсов компьютера;

–осуществлять контроль целостности программных ресурсов компьютера;

–полное окончательное удаление файлов без возможности их последующего восстановления специальными средствами;

–управление печатью документов, простановка автоматических штампов;

–прозрачное шифрование файлов;

–централизованное управление несколькими рабочими станциями с использованием локальной сети;

–возможность использования собственной файловой оболочки, блокирующей использование ряда возможностей;

–блокировка автоматизированного рабочего места посредством использования аппаратных ключей защиты.

Информационные системы:

– 1С: ведение бухгалтерского учета;

– 1С: Зарплата и управление персоналом – расчет зарплаты и ведение кадрового учета.

Работа с остальными информационными системами обеспечивается:

– организационными мерами информационной безопасности;

– аппаратными и программными средствами защиты информации.

Организационные меры безопасности и инженерно-технические решения.

Организационные меры безопасности обеспечены ведением комплекса документации:

– Приказ о назначении администратора информационной безопасности;

– Приказ об утверждении политики информационной безопасности;

– Приказ об утверждении порядка работы с машинными носителями данных;

– Инструкция по работе с информационными системами обработки персональных данных;

– модель угроз.

Модель угроз, необходимо рассмотреть более подробнее, так как нужно определить уровень защищенности. Для определения уровня и требований по обеспечению безопасности информационных ценных ресурсов, а также в

целях определения обоснования внедрения мер по защите ценной информации.

Модель угроз представляет характеристику угроз безопасности информации, описательное представление свойств или характеристик угроз безопасности информации является исходной точкой при разработке контрмер для обеспечения безопасности.

Необходимо отметить, что сформированная в рамках исследования, модель угроз предусматривает системный подход к определению угроз информационной безопасности.

При определении угроз информационной безопасности, были определены как (места размещения оборудования), так и границы информационной системы.

Информационная система развёрнута в помещении строительной конструкции границей которого является контролируемой зоной.

Информационная система состоит локальной сети, которая обрабатывает сведения, различного уровня конфиденциальности, сеть физически взаимодействует посредством коммутатора, и логически разделена посредством межсетевого экрана. Который обеспечивает фильтрацию пакетов.

Результаты идентификации источников угроз определены в таблице 2.

Угрозы реализуются в результате этого осуществляется нарушение свойств информации, которая полежит защите: конфиденциальность, целостность и доступность. Актуальностью угроз определяется тем, что возможности нарушителя достаточны для реализации угрозы информационной безопасности. Модель нарушителя и результаты возможностей (рисунок 6).

Таблица 2 – Источники угроз

Источник угроз	Тип источника угроз	Используемые уязвимости	Способы реализации угроз	Объект ИС	Результат от реализуемой угрозы ИБ
Внутренний нарушитель	Антропогенный	Уязвимости в СЗИ от НСД, недостаток организационно-технических мер	Уничтожение, хищение КИ	Сеть	Нарушение К,Ц,Д
Внешний нарушитель		Недостаток организационно-технических мер	Утечка информации по каналам ПЭМИН	Сеть	Нарушение К
Сбой аппаратно-программного обеспечения	Техногенный	Низкое качество программно-технических средств, охлаждения, электроснабжения технического обслуживания со стороны лиц, выполняющих обслуживание	Утечка информации в результате сбоя оборудования ТС, источники КИ, нарушение целостности, доступности	Сеть	Нарушение К,Ц,Д
Стихийное бедствие	Природное	-	Пожар в помещении	-	Нарушение К, Ц, Д

Таким образом, уровень защищенности, необходимо определить следующим образом:

– по коммуникационному размещению (средний);

– по использованным информационным технологиям (средний);

– по размещению технических средств (низкий);

– по архитектуре информационной системы (низкий);

– по режимам разграничении прав пользователей(низкий);

– по разделению функций управления информационной безопасностью (низкий).

Так как большая часть показателей защищенности имеют «низкий» уровень. Можно сделать вывод о том, что общий уровень защищенности низкий. Поэтому, необходимо рассматривать защитные меры в составе политики информационной безопасности.

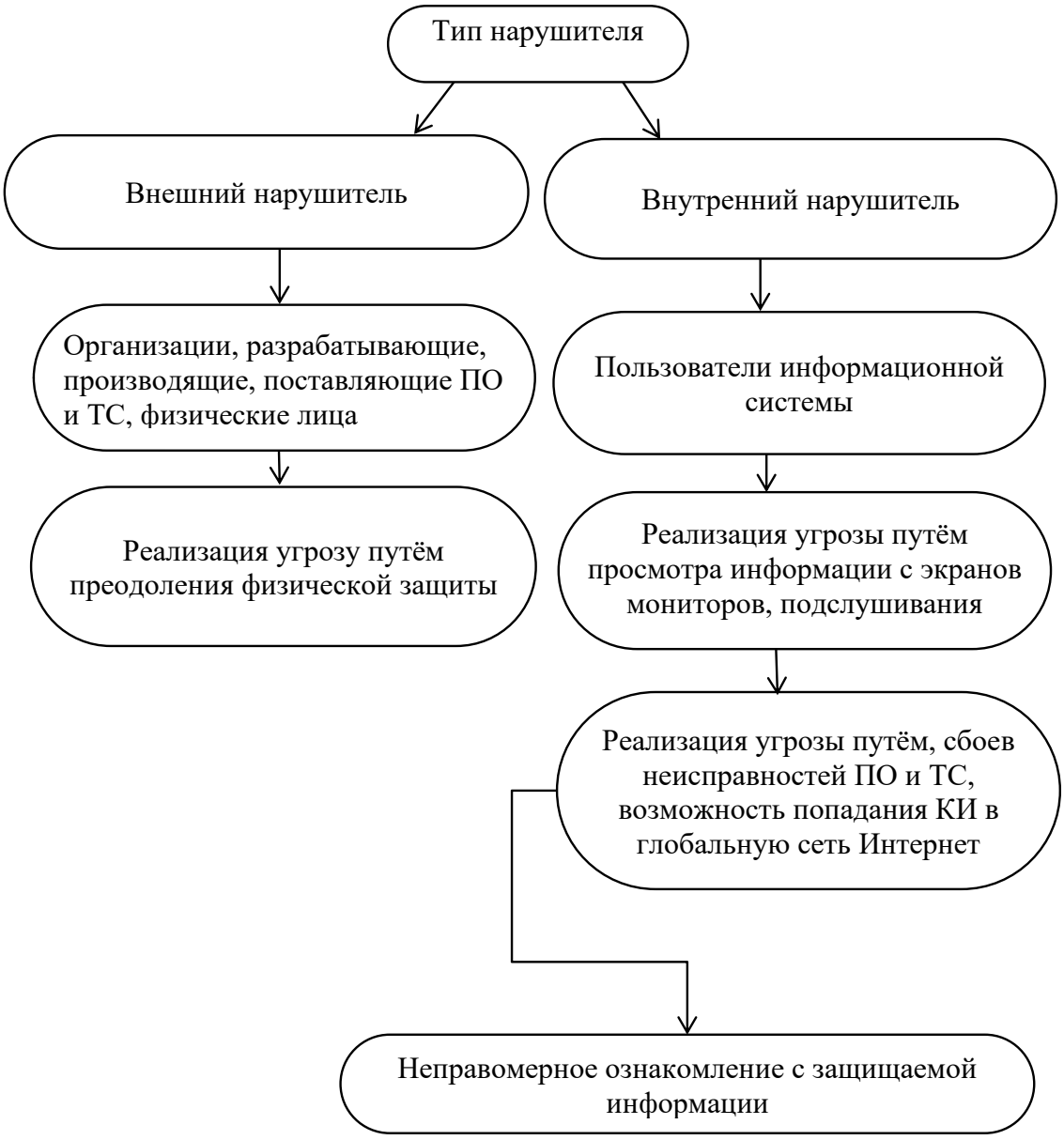

Рисунок 6 - Модель нарушителя

Далее, для хранения серверного оборудования используется отдельно выделенное служебное помещение с ограниченным доступом (металлическая дверь, на окнах располагаются решетки). Все технические помещения (электрощитовая, склад моющих средств, уборное помещение для хранение моющего инвентаря) закрываются на ключ, доступ к ним ограничен рабочим временем в организации.

Инженерно-технический комплекс представлен системой видеонаблюдения, экранированием окон, защитой служебных помещений

(металлические двери, решётки на окнах). Защита конфиденциальных данных и учёта бухгалтерии представлена большим металлическим сейфом, который расположен в кабинете главного бухгалтера.

Для эффективного решения проблем, и решение указанных задач, является централизация потоков с помощью средств централизованной консоли. Для управления информационными потоками предлагается эффективное средство как Межсетевой экран D-Link DFL-870. Это эффективное средство, так как позволяет контролировать трафик и соответственно управлять. Отчеты должны постоянно просматриваться администратором безопасности. Такой подход к обеспечению централизованного управления информационной безопасностью позволит повысить оперативность и эффективность с оптимизацией работы по обеспечению информационной на предприятии ООО «Товаротранспортная компания».

2.2 Разработка комплекса программно-аппаратных средств обеспечения информационной безопасности ООО «Товаротранспортная компания»

На предприятиях различных размеров средства защиты разнообразны и зависят от финансовых возможностей компании. Также разнообразен имеющийся выбор продуктов: средства сетевой защиты (межсетевые экраны), антивирусные решения и другие средства защиты. Очевидно, что без разработки и внедрении средств защиты, стабильное существование хозяйствующего субъекта невозможна.

Поэтому можно утверждать, что средства по обеспечению информационной безопасности входят в состав мер по контролю, а значит и управлению информационной безопасностью.

Итак, рассмотрим ниже перечень мер и средств защиты, использующиеся на предприятии:

– На предприятии принимается недостаточно организационных мер обеспечения безопасности. Отсутствие актов обследования информационных систем приводит к невозможности корректного определения рисков и источников инцидентов информационной безопасности, что приводит к отсутствию четкой стратегии, позволяющий установить необходимый состав программно-аппаратных средств информационной защиты.
– Антивирусная защита основывается на программных средствах, имеющих иное основное предназначение. Так Secret Net Studio имеет в своем составе антивирусные средства, но основное назначение – система мониторинга и предотвращения вторжений. Сетевой экран также имеет собственный антивирусный сканер, но его основное назначение – обеспечение сетевой безопасности при работе в Интернет.
– Использование средства защиты от несанкционированного доступа Dallas Lock имеет часть функций, схожих с Secret Net Studio. При аттестации рабочих мест, как правило, используется либо Secret Net Studio, либо Dallas Lock, но не оба программных средства одновременно. Их одновременное использование приводит к значительному расходованию аппаратных ресурсов, что замедляет выполнение основной работы сотрудниками предприятия.
– Отсутствует выделенное специализированное защищенное место хранения машинных носителей информации.
– Отсутствует документация информационного планирования, что приводит к отсутствию системного подхода к организации процессов:

а) закупки, обновления и замены автоматизированных рабочих мест и офисного оборудования;

б) плановой закупки и обновления средств антивирусной защиты;

в) модернизации и поддержки работоспособности структурной

кабельной сети;

г) обновление и продление лицензий средств криптографической защиты;

д) реализации программы централизованного импортозамещения используемых программных средств.

- В мероприятиях обеспечения информационной безопасности отсутствует перечень разрешенного к использованию программного обеспечения, что позволяет бесконтрольно использовать различное непроверенное и не сертифицированное программное обеспечения.
- Технические сотрудники имеют неконтролируемый доступ в помещения, где используются информационные системы обработки персональных данных. Среди документации информационной защиты отсутствует. Положение о проведение служебных и сервисных работ и График проведения санитарных и технических работ в течение рабочего дня предприятия.
- Коммутаторы D-Link DES 1005D/E располагаются скрытно, в труднодоступных местах, но не установлены в металлические шкафы или специальные стойки, запираемые на ключ.
- Среди технических систем ограничения доступа отсутствует автоматическая сигнализация.

В связи с обнаруженными фактами предлагается использование следующего комплекса программно-аппаратных средств информационной безопасности и дополнительных организационных мероприятий:

- Заменить сетевой шлюз D-Link DFL-870, на Fortigate 30E как обеспечивающий высокую эффективность защиты локальной сети организации от несанкционированного доступа, проникновения и атак извне через сеть Интернет.
- На автоматизированных рабочих местах использовать Secret Net Studio, отказаться от одновременного использования Dallas Lock, так как:

а) одновременное использование обоих систем увеличивает финансовые затраты на обслуживание и обновление обоих комплексов;

б) большинство функций дублируется в обеих системах;

в) использование обеих систем значительно повышает требования к аппаратным ресурсам автоматизированных рабочих мест;

г) суммарная эффективность использования обеих систем не оправдывает временных, трудовых и финансовых затрат.

– Установить российское антивирусное программное обеспечение на каждое автоматизированное рабочее место так как:

а) специализированное антивирусное средство работает эффективней программно-аппаратных комплексов, имеющих другое целевое предназначение;

б) внедрение российского антивирусного программного обеспечения эффективнее использования штатного антивируса операционной системы Microsoft Windows, так как российские разработчики ориентируются на региональные угрозы (возникающие чаще на территории Российской Федерации);

в) внедрение российского антивирусного программного обеспечения соответствует стратегии импортозамещения, принятого правительством Российской Федерации, и облегчит в дальнейшем переход на использование российских операционных систем.

– В качестве средства криптографической защиты необходимо продолжить использование криптопровайдров КриптоПро, так как:

а) они прошли сертификацию ФСТЭК;

б) на их использовании построена работа с электронными подписями и смена криптопровайдеров приведет к необходимости перегенерации электронных ключей;

в) используемые информационные системы способны работать в штатном режиме при использовании ключей, прошедших генерацию

с использованием подсистем КриптоПро;

г) смена криптопровайдера повлечет за собой дополнительные финансовые затраты на приобретение лицензионных прав;

д) КриптоПро поддерживает современные государственные стандарты шифрования и генерации ключей.

– Аппаратные ресурсы автоматизированных рабочих мест на данный момент достаточны для решения большинства повседневных задач. Но в то же время администратору информационной безопасности (или ответственному ИТ-специалисту, в зависимости от распределения обязанностей) необходимо подготовить программу информатизации с включением графика централизованного обновления парка компьютерной техники, так как приближается завершение нормативного срока эксплуатации (с последующим моральным устареванием технических систем).

– Необходимо разработать и утвердить особый порядок использования информационных систем обработки информационных систем с низким уровнем защиты. К таковым относятся:

а) информационные системы на платформе 1С – в файловом режиме работы их использование предполагает бесконтрольный доступ к информационным каталогам посредством использования локальной сети предприятия;

б) СБИС++ – данная информационная система позволяет осуществлять работу с данными с использованием сертификатов безопасности, установленных локально на автоматизированное рабочее место специалиста (без применения внешних контейнеров и ключевых носителей).

– Из-за недостаточно большого числа портов коммутаторов D-Link DES 1005D/E рекомендуется разработать программу их плановой замены на пассивное коммутационное оборудование, имеющее большую скорость передачи данных и большее количество портов.

Это позволит сократить текущее число элементов сетевой инфраструктуры, а также создаст резерв технических систем подключения новых автоматизированных рабочих мест и возможного будущего расширения локальной сети предприятия. В связи с данной рекомендацией ИТ-специалисту предприятия необходимо провести техническую экспертизу структурной кабельной сети для возможного ее изменения с целью использования с новым коммутационным оборудованием.

Для реализации комплексности и минимизации информационных рисков предприятия необходимо применить адаптивные мероприятия, подходящие к любому хозяйствующему субъекту. Приводящие к повышению уровня информационной безопасности. Проводится ниже выбор мероприятий и средств по уменьшению рисков. Мероприятия для обеспечения безопасности информационных важных информационных ресурсов предприятия состоят из двух модулей: Программно-технические средства и организационные.

В перечень организационных мероприятий для обеспечения безопасности информационных важных информационных ресурсов входит:

– на основе бизнес-целей предприятия, создание политики информационной определяющей управление ИБ;

– установление режима информационной безопасности в соответствии с требованиями действующего законодательства, использование мировой практики;

– назначение ответственных за обеспечение ИБ;

– определение ответственности за невыполнение правил по обеспечению ИБ;

– включение в должностные инструкции обязанности по соблюдению режима ИБ;

– разграничение доступа к информации в соответствии со служебной необходимостью;

– осуществление проверочных мероприятий при приеме сотрудников на работу;

– обучение сотрудников вопросам обеспечения ИБ, процедурам защиты и правильного обращения с информационными ресурсами предприятия;

– подписание с работниками обязательства о неразглашении конфиденциальной информации;

– ознакомление сотрудников с действующими в организации нормативно правовыми документами в сфере обеспечения ИБ;

– организация пропускного режима;

– установление правил обработки, использования, распространения и хранения документов;

– разработка перечня конфиденциальных сведений;

– разработка правил эксплуатации ИС, доведение их до сотрудников, контроль за их выполнением;

– назначение ответственных за администрирование компьютеров и сети;

– определение процедур использования и хранения носителей информации;

– ознакомление сотрудников с процедурой уведомления руководства о различных типах инцидентов (нарушения безопасности, сбои в работе и т.п);

– планирование бесперебойной работы предприятия для максимально быстрого восстановления процессов обработки информации.

Для реализации комплексности, необходимо на предприятии создать постоянно действующую группу. Данная группа сотрудников предназначена для выработки правил, рекомендаций руководству предприятия, направленных на эффективное управление информационной безопасностью, обнаружение и устранение возможных каналов утечки ценной информации, организацию и координацию работ по совершенствованию защиты. Ниже приведен состав ПДГ, ее нормативно-организационный статус и спектр задач, которые она должна решать.

Состав должен состоять из:

– Генерального директора предприятия;

– Менеджера;

– Юриста;

– Экспедитора логиста;

– Бухгалтера;

– ИТ-специалиста (администратора безопасности).

Нормативно-организационный статус ПДГ предполагает, что она должна подчиняться генеральному директору предприятия, так на данном предприятии несет ответственность за соблюдение правил обращения с конфиденциальной информацией.

ПДГ отвечает за:

– разработку и издание инструкций (правил) по обеспечению безопасности, соответствующих общим правилам работы предприятия и требованиям к обработке информации;

– классификацию степени конфиденциальности информации;

– разработку и обеспечение выполнения программы обучения и ознакомления с основами ИБ в масштабах организации;

– разработку и сопровождение перечня минимальных требований к процедурам контроля за доступом ко всем ПК;

– проверку и отбор соответствующих методик планирования восстановления работы, принимающих участие в автоматизированной обработке ценной информации;

– разработку и внедрение процедур пересмотра правил обеспечения ИБ, а также рабочих программ, предназначенных для поддержки правил, инструкций;

– участие в описании, приобретении различных информационных систем в целях соблюдения требований безопасности;

– оценку и выбор для внедрения аппаратных и программных средств, оборудования.

Перечень типовых задач ПДГ отражает основную задачу управления ИБ предприятия - она определяет направления развития и поддержки усилий предприятия, направленных на защиту информации от несанкционированных действий и отказа в доступе. Это достигается путем внедрения соответствующих инструкций, правил. Внедрение комплексного подхода невозможно без нормальной организации работы ПДГ.

Вышеуказанные мероприятия указывают на то, что задача по повышению уровня информационной безопасности на предприятии- выполнена.

2.3 Разработка инженерно-технического мер обеспечения информационной безопасности ООО «Товаротранспортная компания»

Исходя, из анализа защиты описанном выше предлагается внедрение следующих мероприятий:

– Коммутационное оборудование необходимо установить в специализированные стойки или металлические шкафы с замками, запираемыми на ключ.

– Провести техническую экспертизу структурной кабельной сети с целью обнаружения возможности монтажа сетевого кабеля скрытым способом, вне прямой доступности персонала и клиентов (под потолком, в технических помещениях, в технических магистралях).

– Необходимо выделение специализированного места хранения машинных носителей информации (запираемый металлический шкаф или сейф). Необходимо провести ревизию документационного обеспечения процесса использования машинных носителей информации (составить инструкции сотрудников, имеющих право использовать машинные носители, завести журнал учета выдачи машинных носителей информации, составить график доступа и список лиц, имеющих доступ к специализированному месту

хранения машинных носителей информации).

– Администратору информационной безопасности необходимо разработать план проверки инженерно-технических средств информационной защиты, в котором отразить:

а) периодичность проверки;

б) проверку соответствии автоматизированного рабочего места сведениям аттестационного листа;

в) проверку соответствия помещений сведениям аттестационного листа;

г) проверку средств видеонаблюдения;

д) проверку технического состояния и исправности металлических дверей, стоек с оборудованием и металлических шкафов, в которых хранятся машинные носители информации, сертификаты и парольно-ключевая информация на бумажных носителях, документация, содержащая персональные данные и конфиденциальные сведения;

е) проверку технического состояния активного и пассивного коммутационного оборудования сетевой инфраструктуры предприятия;

ж) выполнения комплекса мероприятий по поиску мест установки средств аудио и визуального съема информации;

з) проверку логов сетевого шлюза на предмет обнаружения проникновения извне;

и) анализ инцидентов по журналу учета инцидентов безопасности.

– Выполнить комплекс мероприятий по контролю систем доступа к помещениям, в которых выполнена аттестация рабочего места и установлены информационные системы обработки персональных данных (проверка документации, списки лиц, имеющих доступ, выяснение местонахождение ключей и магнитных карт и т. д.).

– Рассмотреть комплекс мер по введению систем аппаратного и программного копирования сведений информационных систем обработки персональных данных (там, где имеется такая возможность). Среди таких систем:

а) информационные системы на платформе 1С;

б) система электронного документооборота и сдачи отчетности СБИС++.

Данные мероприятия необходимо внести в состав комплексных мер, так как инженерно-техническая защищенность, является одним из ключевых направлений по обеспечению информационной безопасности.

2.4 Выбор эффективных средств управления средств защиты информации ООО «Товаротранспортная компания»

Организация и поддержание информационной безопасности предприятия представляет собой комплекс решений в различных направлениях. Поэтому, для обеспечения полноценного использования криптографических средств защиты данных, необходимо их полноценное организационное и документационное обеспечение.

Документационное сопровождение средств защиты персональных данных представляется следующими локальными актами предприятия:

– Положение о парольной защите – содержит общие сведения об организации парольной защиты, порядке генерации и уничтожении парольно-ключевой информации.

– Приказ об утверждении политики информационной безопасности – документ, утверждающий основные положения организации информационной безопасности. Содержит общие положения использования криптографических средств защиты информации.

– Приказ об организации работ по обеспечению безопасности персональных данных. Локальный акт, в котором отражается информация о порядке обработке персональных данных, о порядке использования информационных систем, о порядке применения средств криптографии и электронных ключей;

– Технический паспорт информационной системы – помимо

различных технических сведений содержит порядок применения парольно-ключевой информации, сертификатов безопасности и электронных подписей;

– Инструкция о порядке работы с персональными данными – содержит организационные положения организации защиты персональных данных с использованием различных программных и аппаратных средств;

– Правила обработки персональных данных – представляет собой документ, содержащий требования к процессу организации обработки персональных данных как с использованием информационных систем (в совокупности с криптографическими системами), так и без средств автоматизации (с хранением парольно-ключевой информации на бумажных носителях);

– Инструкция администратора информационной безопасности. Представляет собой документ, в котором отражаются общие направления работы администратора информационной безопасности, одним из которых является работа со средствами криптографической защиты информации;

– Журнал учета средств защиты информации. Представляет собой реализацию требования ведения учета средств информационной защиты. Содержит основные сведения о получении средств защиты информации, ответственных за хранение и использовании, дате обновления, дате генерации сертификатов и электронных подписей;

– Журнал учета паролей информационной системы. Используется для накопления сведений о централизованной генерации и выдачи паролей информационных систем обработки персональных данных, используемых на предприятии;

– Акт уничтожения электронной подписи. Представляет собой документ, подтверждающий факт уничтожения электронной подписи. В соответствии с порядком уничтожается сертификат электронной подписи, закрытый ключ. В зависимости от класса защиты может также уничтожаться и машинные носители электронных подписей.

Администратору информационной безопасности предприятия

рекомендуется провести ревизию используемого документационного обеспечения и привести его в соответствии с требованиями законодательства Российской Федерации.

Основу программных средств криптографической защиты информации представляет собой комплекс программного обеспечения Крипто Про. На данный момент криптопровайдер полностью соответствует ГОСТ 34.10-2018 «Информационная технология. Криптографическая защита информации. Процессы формирования и проверки электронной цифровой подписи» и имеет сертификат ФСЭК, может использоваться для организации различного класса защищенности.

Особенность комплекса Крипто Про это блочная структура, благодаря чему пользователь может гибко настроить свою работу, в зависимости от потребностей и необходимого уровня криптографической защиты. В то же время, на предприятии востребована только часть функций криптопровайдера:

– генерация ключей;

– авторизация при входе в информационные системы (включая государственные информационные системы);

– подписание электронных документов.

В целом на предприятии развернута достаточно эффективная работа со средствами криптографической защиты, однако необходимо провести комплекс мероприятий по ревизии документарного обеспечения.

2.5 Разработка методики анализа программного обеспечения технических средств с целью обнаружения возможности возникновения угроз процессам информационной безопасности

В рамках данной работы разработка методики анализа программного обеспечения технических средств для реализации защиты информационных процессов ООО «Товаротранспортная компания», входит в состав технических мер области обеспечения информационной безопасности. Целью

данной методики, является определение возможности возникновения опасных событий (инцидентов), которые влияют на уровень защиты, за счет отклонений (сбоев) от штатного алгоритма функционирования технических средств. Реализация которых может повлиять на процесс управления информационной безопасностью.

Результаты анализа по разработанной методике были использованы для уточнения вероятности возникновения опасных событий в ООО «Товаротранспортная компания», за счет неисправностей (сбоев) исследуемого технического средства, что является практическим опытом в рамках исследовательской работы.

Для анализа были выбраны: АРМ 1, АРМ 2 (коммутатор). Анализ аппаратного обеспечения технического средства приведен на примере АРМ1. Указанное изделие — это автоматизированное рабочее место менеджера по продажам, чтобы автоматизировать задачи.

Аппаратный блок АРМ 1 выполнен на базе ПЭВМ, имеется ЖК монитор, проводная «мышь» и клавиатура (рисунок 7).

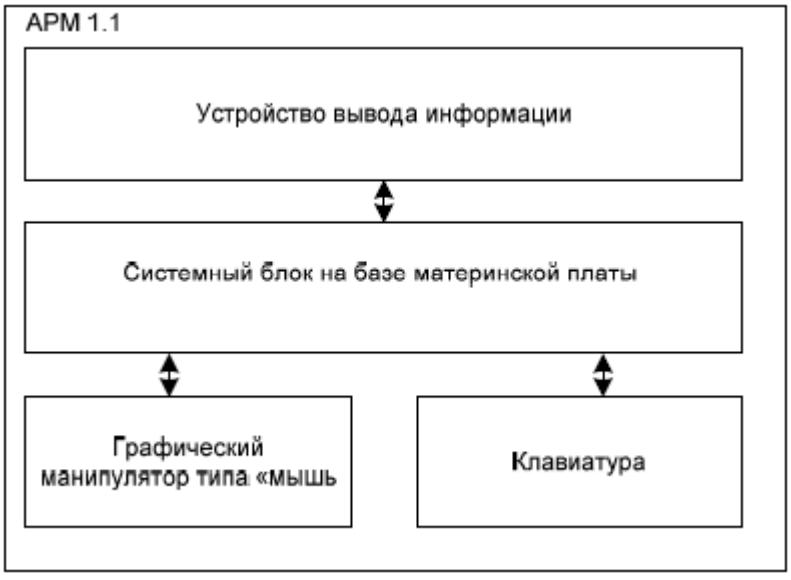

Рисунок 7 - Состав устройств АРМ 1

Далее, рассмотрим неисправности и сбои, которые могут примести к

возникновению опасных событий.

Неисправности и сбои микросхем центрального процессора могут привести к ошибочному выполнению команд. Неисправности и сбои накопителя могут привести к искажению команд. Неисправности и сбои сетевых адаптеров к могут привести к искажению при передаче данных в локальной сети, что может привести к возникновению опасных событий.

Следовательно, опасные события могут привести к неисправности или сбою, следящих изделий - (CPU), накопитель и сетевой адаптер.

В процессе обмена данными АРМ 1 взаимодействует с АРМ 2 используются принципы сетевого взаимодействия на базе протокола TCP/IP. Чтобы обеспечить обмен используется протоколы сетевой модели OSI:

– физическом и канальном уровне;

– на сетевом уровне;

– на транспортном уровне.

Пакет сообщения включает заголовки: Ethernet; IP; UDP.

Таким образом, в процессе взаимодействия устройств, осуществляющих обмен конфиденциальными сообщениями и не конфиденциальными.

В сообщениях данных содержаться фрагменты документов конфиденциального и не конфиденциального характера.

В сообщениях обмена имеются поля, в которых могут содержаться данные из множества значений. В результате искажения полей заголовка пакета (код узла – отправителя), структура поля может измениться или вообще отсутствовать вследствие чего, возможно возникновений опасных для информационной системы событий. Которые влияют на обеспечение информационной безопасности.

Для понимания циркуляции процесса информационных потоков была представлена схема (рисунок 8).

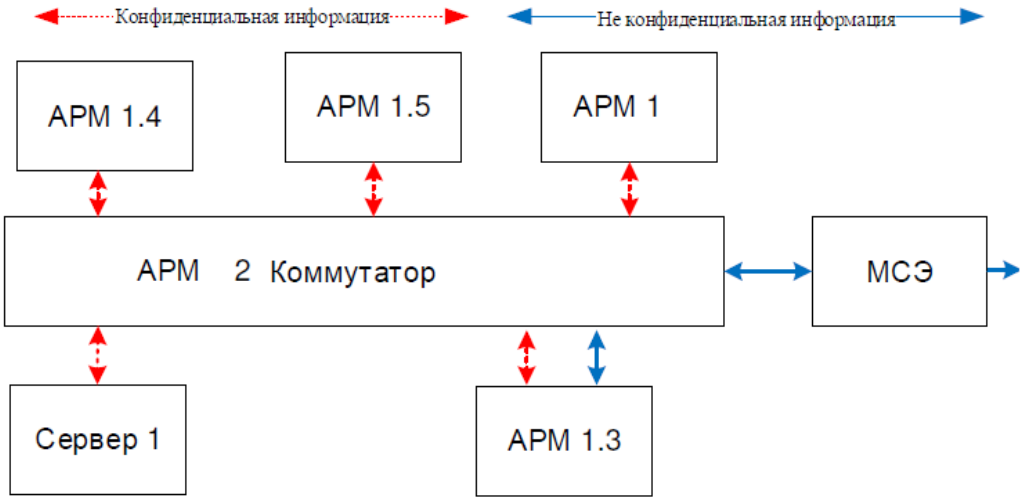

Рисунок 8 - Схема информационных потоков между АРМ1, АРМ2

В процессе передачи конфиденциальной информации, за счет сбоев и неисправностей возможно формирование искаженного, ошибочного пакета данных - коммутатор передаст штатно на сервер. Данные также могут попасть в глобальную сеть Ethernet.

Таким образом, можно сделать вывод, что опасным событием будет являться реализация актуальной угрозы для информационной системы технических средств при обеспечении информационной безопасности.

В связи с этим появляется необходимость в разработке методики анализа программного анализа программного обеспечения технических средств в ООО «Товаротранспортная компания», которую можно условно разделить на восемь этапов:

– описание состава программного обеспечения технических средств;

– описание процесса сборки и развертывания программного обеспечения;

– описание и анализ протоколов взаимодействия технических средств в составе информационной инфраструктуры;

– выбор модулей из состава ПО для анализа;

– восстановление алгоритма программы;

– разработка схемы восстановленного алгоритма программы;

– формирование выводов по результатам анализа программного обеспечения.

В процессе выполнения первого этапа анализа программного обеспечения, согласно разработанной методике, необходимо составить перечень всего программного обеспечения, а также описать функциональные задачи специального программного обеспечения и перечня его программных модулей.

Результатами выполнения данного этапа являются следующие сведения:

– сформирован перечень программного обеспечения;

– встроенного, системного, функционального, специального входящего в состав технических средств, с указанием децимальных номеров и сведений о сертификатах соответствия;

– краткое описание функциональных задач программного обеспечения, отражающее взаимодействие технических средств для классификации средств по назначению. На данном этапе рассматриваются функциональные задачи программного обеспечения, отражающее взаимодействие технического средства в составе технического обеспечения предприятия, так как от программного обеспечения зависит нормальное функционирование комплекса технических средств;

– сформирован перечень программных модулей СПО с кратким описанием назначения этих модулей.

В процессе выполнения второго этапа анализа программного обеспечения, согласно разработанной методике, необходимо выполнить фиксацию версии исследуемого программного обеспечения, провести сборку и развертывание программного обеспечения. Для выполнения данного этапа анализа можно воспользоваться UML-диаграммой последовательности действий, выполняемых в процессе сборки и развертывания программного обеспечения в информационном инструкторе (рисунок 9).

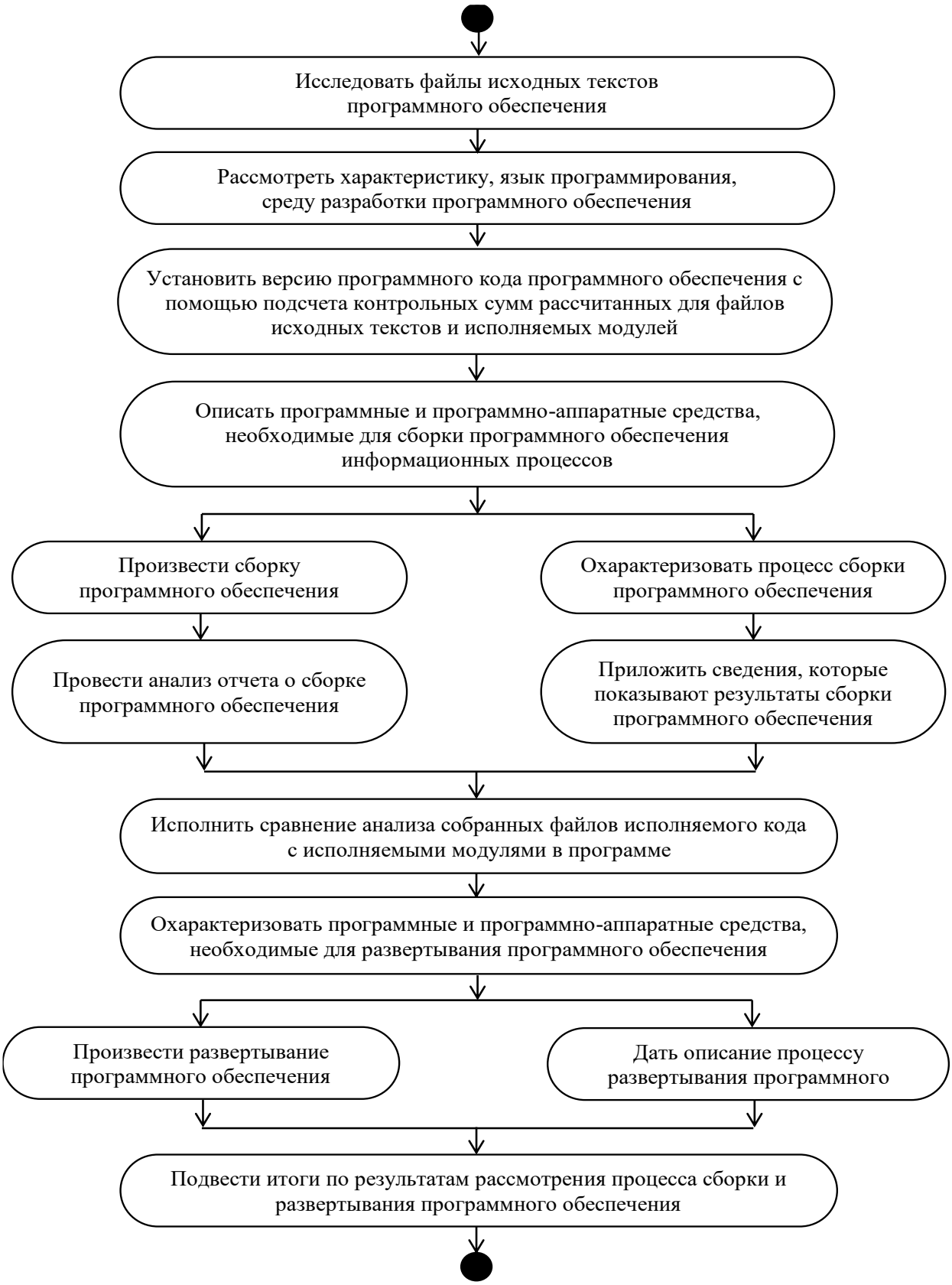

Рисунок 9 – UML-диаграмма последовательности действий, выполняемых в процессе сборки и развертывания программного обеспечения

Результатами выполнения данного этапа являются следующие сведения:

– о версии специального программного обеспечения, языке программирования, среде разработки и выполнения специального программного обеспечения;

– о программных и аппаратно-программных средствах, необходимых для сборки специального программного обеспечения;

– о результатах сборки, а также о соответствии собранного специального программного обеспечения;

– о средствах, методах, процедурах, используемых при развертывании специального программного обеспечения;

– об ошибках компиляции (при наличии).

В процессе выполнения третьего этапа анализа программного обеспечения, согласно разработанной методике, необходимо описать и проанализировать протоколы взаимодействия технических средств. Результатами выполнения данного этапа являются следующие сведения:

– перечень технических средств, с которыми взаимодействует исследуемое техническое средство, с описанием физической среды сопряжения и механизмов обмена данными;

– описание формата информационных сообщений, с указанием назначения каждого поля и перечня значений, которые могут содержаться в этих полях;

– информация о наличии (отсутствии) в полях сообщений обмена значений, которые могут приводить к возникновению опасных событий, определенных для информационной инфраструктуры.

В процессе выполнения четвертого этапа анализа программного обеспечения, согласно разработанной методике, необходимо описать принципы работы, тракты прохождения информации, и провести анализ взаимодействия функциональных компонент (подпрограмм). Результатами выполнения данного этапа являются следующие сведения:

– описание принципов работы исследуемого технического средства в

режиме работы программного обеспечения с указанием перечня транспортных средств, с которыми оно взаимодействует;

– схема взаимодействия программ программного обеспечения, которая должна содержать все основные программные компоненты и их взаимосвязи, отражающие прохождение информации различного типа (конфиденциальной, не конфиденциальной, служебной).

– описание схемы взаимодействия программ с указанием используемых модулей и основных функциональных задач (прием, обработка, формирование и передача сообщений);

– перечень модулей, выбранных по результатам анализа схемы взаимодействия подпрограмм для восстановления алгоритма работы программы, путем пооператорного анализа этих модулей.

На пятом этапе анализа программного обеспечения, согласно разработанной методике, необходимо восстановить алгоритм работы программы путем пооператорного анализа текстов (исходного кода) программных модулей, выбранных в результате выполнения предыдущего этапа анализа. Для выполнения данного этапа анализа можно воспользоваться UML-диаграммой последовательности действий, восстановления алгоритма программы (рисунок 10).

Результатами выполнения данного этапа являются следующие сведения:

– перечень основных механизмов взаимодействия программных компонент и описание программного модуля, содержащего точку входа в программу, описание основной функции программы и разработанный псевдокод этой функции;

– перечень основных функциональных задач, реализованных в программном обеспечении технических средств, и описание восстановленного алгоритма работы основных функциональных задач программного обеспечения, с указанием функций, участвующих в процессе выполнения основной ветки алгоритма и их описания. Разработка схем (граф) вызовов функций подзадачи.

Рисунок 10 – UML-диаграмма последовательности действий при восстановлении алгоритма ПО

На шестом этапе анализа программного обеспечения, согласно разработанной методике, необходимо провести анализ восстановленного алгоритма работы на предмет определения возможных последствий в результате отклонений от штатного алгоритма в процессе выполнения функциональных задач программного обеспечения. Результатом выполнения данного этапа является перечень основных функциональных задач с указанием худших последствий отклонения от штатного алгоритма в процессе решения этих задач

На седьмом этапе анализа программного обеспечения, согласно разработанной методике, необходимо разработать схему восстановленного на предыдущем этапе алгоритма работы программы технического средства. Результатом выполнения данного этапа является схема восстановленного алгоритма работы выбранных модулей программы, с указанием на ней критичных, приводящих к возникновению опасных событий подпрограмм.

На восьмом этапе анализа программного обеспечения, согласно разработанной методике, необходимо сделать выводы по результатам анализа программного обеспечения. В выводах необходимо отразить информацию (при наличии) о выявленных в процессе анализа программного обеспечения опасных программных конструкциях, ошибочно реализованных протоколах информационно- логического взаимодействия, об ошибках совместимости программного обеспечения и др. ошибок программного обеспечения, обнаруженных при пооператорном анализе, а также при анализе с использованием средств статического анализа исходного кода.

В результате выполнения данного этапа необходимо определить возможность (невозможность) возникновения опасных событий информационной структуры компании, в результате отклонения технического средства от штатного режима функционирования. Для наглядного представления описанной методики была разработана UML- диаграмма последовательности действий анализа программного обеспечения технического средства (рисунок 11).

Рисунок 11 – UML-диаграмма последовательности действий при анализе программного обеспечения технического средства

Результаты анализа по разработанной методике рекомендуется использовать для уточнения вероятности возникновения опасных событий для информационной инфраструктуры в хозяйствующем субъекте ООО «Товаротранспортная компания», за счет неисправностей (сбоев) исследуемого технического средства.

На основании результатов анализа программного обеспечения информационной инфраструктуры в составе информационной системы, сформулированы и рекомендованы мероприятия по доработке программно-аппаратного обеспечения технического средства в целях снижения вероятности возникновения опасных событий.

Таким образом, можно прийти к выводу, что результаты разработанной методике, для определения возможности возникновения событий представляющую опасность. Вышеуказанные результаты могут применяться на практике при анализе информационной инфраструктуры на предприятии на соответствие требованиям по обеспечению информационной безопасности.

Хотелось бы подчеркнуть, что опасное событие, может реализоваться (событие) представляющее угрозу информационной безопасности.

2.6 Анализ рисков и оценка для обеспечения управления информационной безопасность

Оценка информационных рисков представляет собой одной из главных направлений достижения риск защищённости предприятия. С помощь, которой можно наблюдать уровень защищенности. Приходится считать, что многие подходы к обеспечению защищенности информационных активов предприятий, зафиксированные в определенных руководящих документах, стандартах, рассматривают во многом технические и технологические аспекты, которые на нынешнем этапе являются наиболее изученными.

Однако, другие некоторые вопросы, зачастую выпадают из рассмотрения, такие как непрерывный контроль за функционированием всей

системы защиты информационных активов, включающею в себя сотрудников предприятия, и оценку степени надежности сотрудников в работе, связанной с ценными информационными ресурсами.

Поэтому, сегодня требуется формирование современных методических подходов в сфере оценки защищенности ценных информационных ресурсов для повышения уровня управления информационной при защите.

С учетом поставленных задач, будет проведен анализ и разработана методика для просчета рисков, которые могут произойти.

Применив приведенную методику на реальном предприятии ООО «Товаротранспортная компания», будут проанализированы выводы.

Расчёт рисков в соответствии с методикой необходимо начинать проведением с мероприятий, результат будет отчет с суммарными результатами всех мероприятий по оценке степени рисков на предприятии. В нашем случае рассматривается корпоративная информационная система, имеющая доступ к глобальной сети интернет. Активы имеющую ценность для предприятия необходимо поделить на основные и вспомогательные (рисунок 12).

В первую очередь, основные активы необходимо определить их ценность для предприятия.

Предлагается рассмотреть с помощью бальной системы, состоящей из 4-х баллов:

- Реализация риска, направленного на целостность, доступность или конфиденциальность и не будет иметь последствий, в целом для предприятия и в частности бизнес-процессов;
- Реализация риска, направленного на целостность, доступность или конфиденциальность, приведет к незначительным потерям для предприятия, в условиях, когда восстановление до первоначального состояния возможно не останавливая бизнес-процессов;
- Реализация риска, направленного на направленного на целостность, доступность или конфиденциальность приведет к значительным

финансовым потерям или окажет негативное существенное влияние на репутацию предприятия, в условиях, когда восстановление до первоначального состояния возможно, но требует больших финансовых затрат или временных;

– Реализация риска, направленного на целостность, доступность или конфиденциальность приведет к полной приостановке бизнес-процессов, окажет негативное значительное влияние к существенным финансовым потерям и на репутацию предприятия.

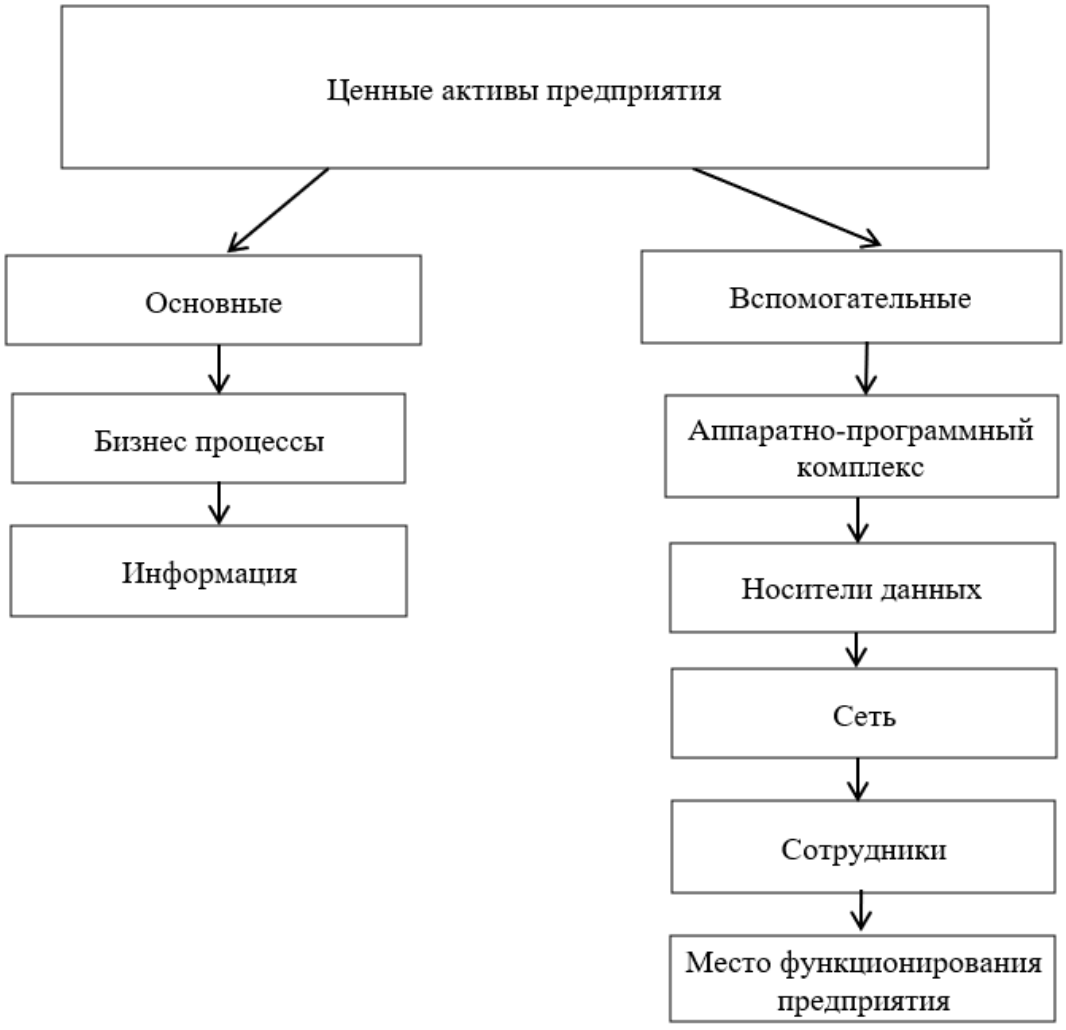

Рисунок 12 – Схема основных и вспомогательных активов

Главной особенностью является то, что основной ущерб бизнес-процессам предприятия способны нанести угрозы доступности к коммутаторам, маршрутизаторам и программно-аппаратному обеспечению, а не угрозы, направленные на нарушение конфиденциальности ценной информации.

В таблице 3 представлены шкалы ценности активов предприятия. На основании указанной таблицы можно производить категорирование.

Таблица 3 – Таблица ценности активов предприятия

Идентификатор	Актив предприятия		Конфиденциальность	Целостность	Доступность	Ценность актива
A	Основные активы	Сведения, необходимые для реализации назначения предприятия	3	4	4	3
B		Сведения личного (конфиденциального) характера	4	2	2	2
C		Стратегические сведения, необходимые для достижения целей предприятия	3	2	2	3
D		Сведения, на обработку которых требуются продолжительное время и связано с большими затратами	2	2	2	3
E	Аппаратно-программный комплекс		–	3	4	4
F	Носители информации		–	1	2	2
G	Сеть		–	3	4	3
H	Сотрудники		–	1	2	1
I	Место функционирования предприятия		–	2	1	2

Теперь рассмотрим оценку рисков информационной безопасности предприятии ООО «Товаротранспортная компания».

Обработку рисков необходимо рассматривать, как повторяющиеся действия (итеративный) процесс, что позволяет повысить уровень детализации оценки рисков при каждой следующей стадии повторения. За основу представлен пример (рисунок 13), повторяющегося действия

(итеративного) процесса оценки и обработки рисков. Контекстом риска можно понять, как установление критериев для обработки рисков, а также назначаются ответственные работники, занимающиеся вопросами обеспечения безопасности в нашем, случает, это постоянно действующая группа.

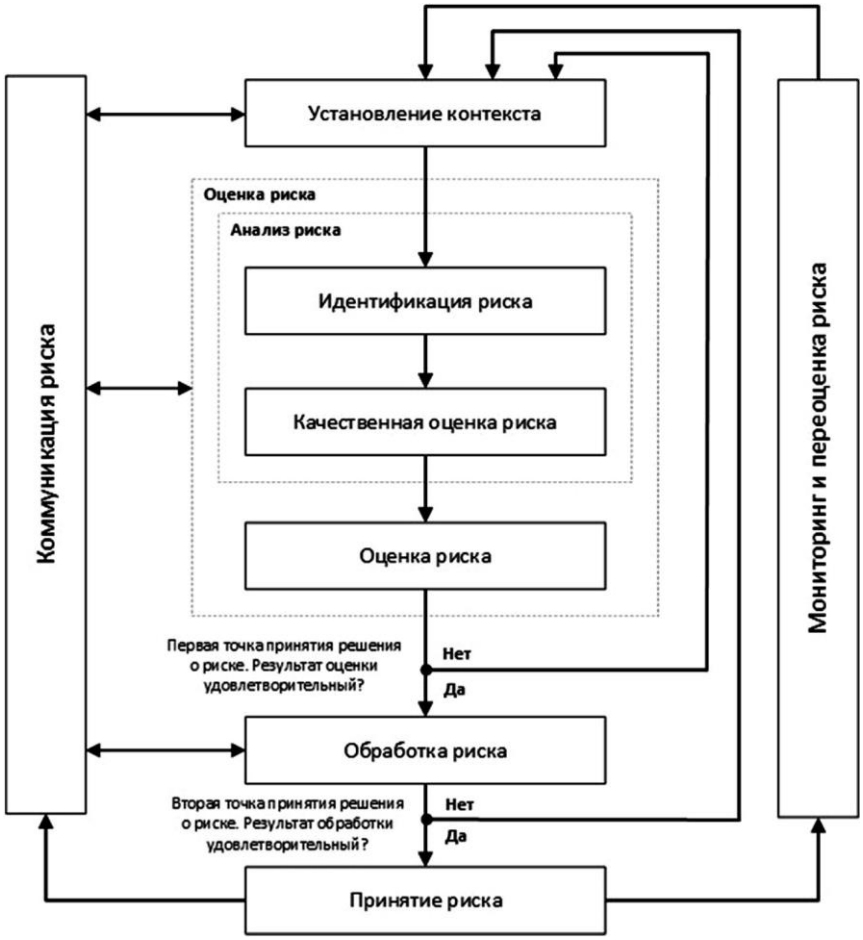

Рисунок 13 - Процесс обработки и анализа оценки рисков

Идентифицировать риск необходимо как процесс нахождения и определения рисков. Оценкой риска понимается присвоение значений последствиям реализации риска и вероятности его реализации. Под принятием риска понимается, что ущерб от реализации риска является оптимальным, а вероятность его реализации низкая, что позволяет не проводить процедуры обработки риска. Коммуникация риска осуществляет обмен сообщениями об

актуальных рисках между сторонами. Под обработкой риска понимается как процесс минимизации вероятности реализации риска или процесс минимизации последствий от реализации риска. Пример деятельности по обработке рисков (рисунок 14).

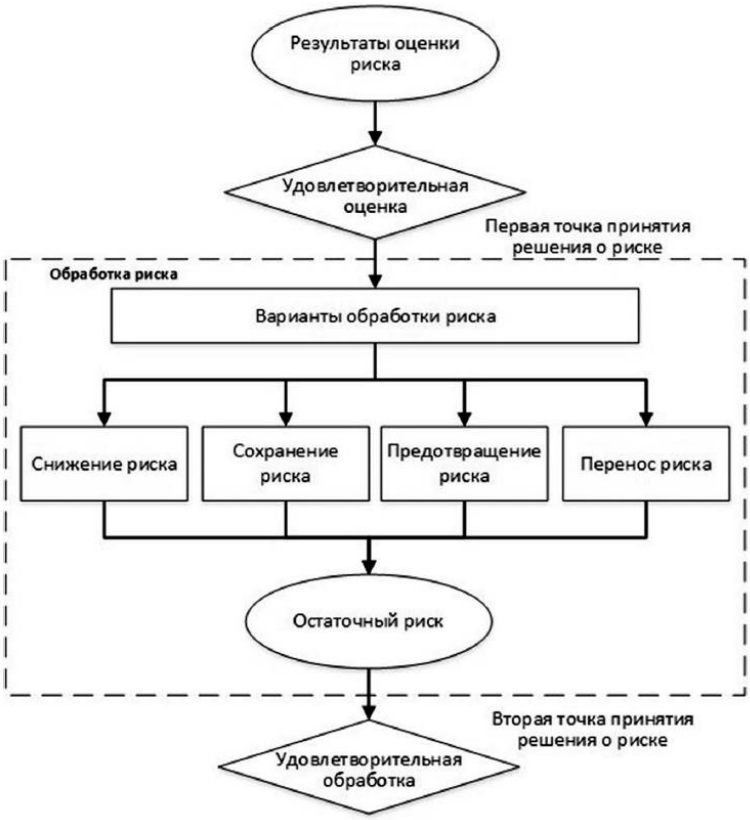

Рисунок 14 - Пример деятельности по обработке рисков информационной безопасности

Следующим действием, является определение степени уязвимости каждого из ценных активов предприятия. В соответствии ФСТЭК банком данных угроз будет рассмотрен выборочный перечень угроз (рисунок 15).

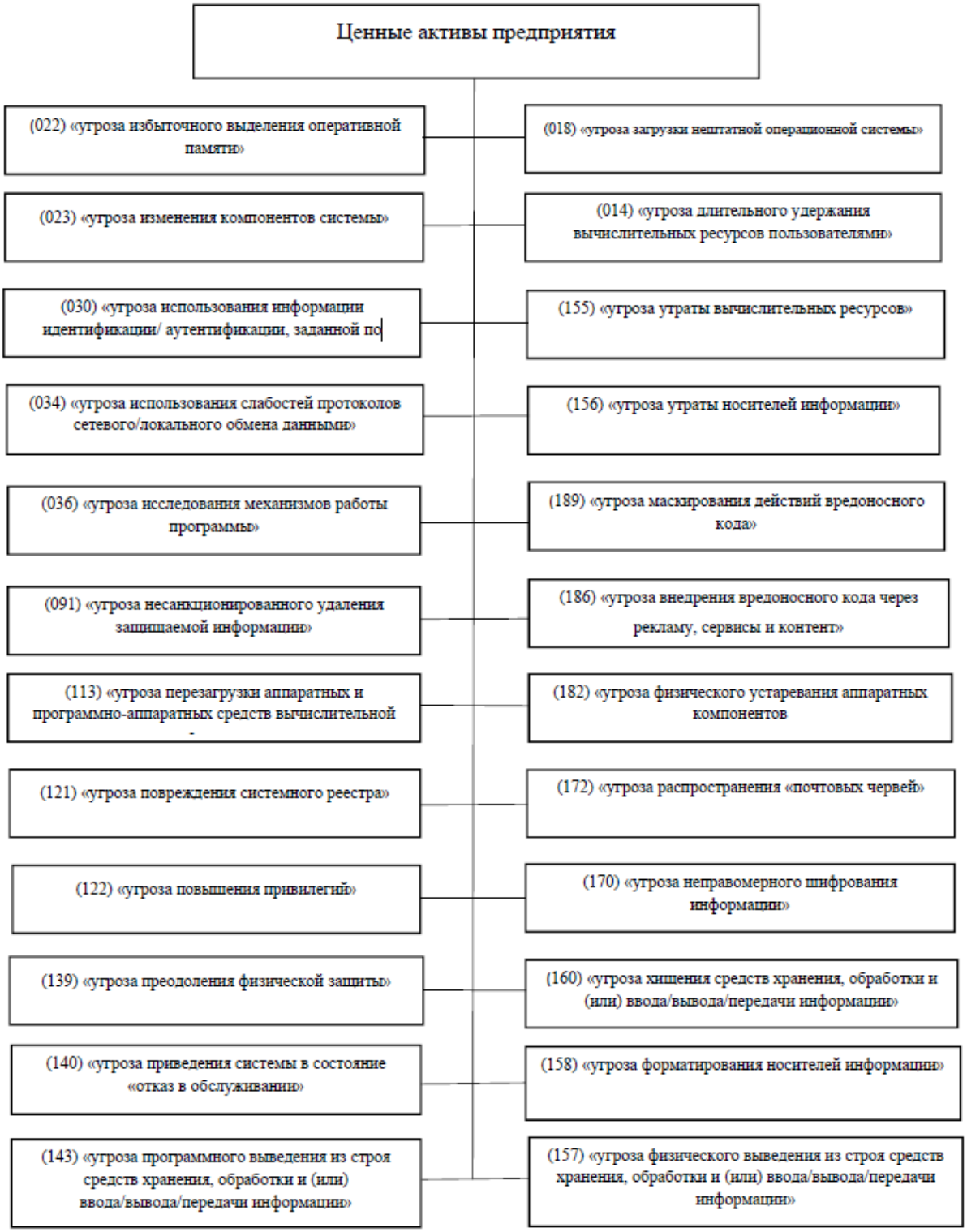

Рисунок 15 – Выборочный перечень угроз

В результате, был сформирован отчет, об оценке рисков информационной безопасности (рисунок 16).

Ценный актив компании	Угрозы	ЦН	СУ	В	Р	Числовое значение оценки риска
Сведения, необходимые для реализации назначения или бизнеса компании	018	4	1	1	4	Низкий
	030	4	2	1	8	Низкий
	036	4	1	2	8	Низкий
	091	4	3	4	48	Высокий
	121	4	2	2	16	Средний
	139	4	1	3	12	Средний
	143	4	3	2	24	Высокий
	155	4	1	2	8	Низкий
	156	4	3	4	48	Высокий
	158	4	1	3	12	Низкий
	160	4	1	3	12	Низкий
	170	4	2	2	16	Низкий
	186	4	2	3	24	Высокий
Аппаратно-программный комплекс	014	4	2	2	16	Средний
	018	4	3	1	12	Средний
	022	4	2	2	16	Средний
	023	4	3	3	36	Высокий
	030	4	1	1	4	Низкий
	036	4	1	2	8	Низкий
	113	4	2	2	16	Средний
	121	4	2	2	16	Средний
	122	4	2	2	16	Средний
	139	4	3	3	36	Высокий
	140	4	3	2	24	Высокий
	143	4	2	2	16	Средний
	155	4	3	2	24	Высокий
	157	4	1	3	12	Средний
	160	4	2	3	24	Высокий
	182	4	1	3	12	Средний
	189	4	1	2	8	Низкий
Сеть	022	4	2	2	16	Средний
	034	4	1	2	8	Низкий
	036	4	1	2	8	Низкий
	140	4	3	2	24	Высокий
	155	4	3	2	24	Высокий
	172	4	2	2	16	Средний
	182	4	1	3	12	Средний
	186	4	2	3	24	Высокий
	189	4	1	2	8	Низкий

Рисунок 16 – Отчет об оценки рисков при обеспечении информационной безопасности ООО «Товаротранспортная компания»

Общий уровень риска информационной безопасности на предприятии ООО «Товаротранспортная компания» для каждого из ценных активов на предприятии рассчитывался по формуле 1

$$A, E, G. P = ЦН \times СУ \times В \quad (1)$$

На рисунок 16 в представлен результат для активов предприятия. Приемлемым риском считается риск, если значение находится в промежутке от 1 до 10, данный риск считается незначительным и обработка данного риска не требуется. Средний риск, если значение находится в диапазоне от 11 до 21, то рекомендуется к обработке с целью его минимизировать. Высокий риск, если значение находится в диапазоне от 22 до 64, данный риск считается значительным и его обработка необходима.

В ходе анализа полученных результатов и обработка такого риска. Было установлено, что в некоторых категориях значение находится в диапазоне от 11 до 21 рекомендуется к обработке для его минимизации. Высокий риск, если значение находится в диапазоне от 22 до 64, данный риск считается значительным, и его обработка обязательна.

В результате расчётов, которые показали угрозы:

– Угроза (014) – диапазон (высокая);

– Угроза (018) – диапазон (средняя);

– Угроза (022) – диапазон (средняя);

– Угроза (023) – диапазон (высокая);

– Угроза (030) – диапазон (средняя);

– Угроза (014) – диапазон (высокая);

– Угроза (014) – диапазон (высокая);

– Угроза (036) –диапазон (средняя);

– Угроза (034) – диапазон (высокая);

– Угроза (091) – диапазон (высокая);

– Угроза (113) – диапазон (высокая);

– Угроза (122) – диапазон (высокая);

– Угроза (121) – диапазон (средняя);

– Угроза (139) – диапазон (высокая);

– Угроза (140) – диапазон (средняя);

– Угроза (143) – диапазон (средняя);

– Угроза (155) – диапазон (низкая);

– Угроза (156) – диапазон (высокая);

– Угроза (157) – диапазон (высокая);

– Угроза (158) – диапазон (средняя);

– Угроза (160) – диапазон (высокая);

– Угроза (170) – диапазон (средняя);

– Угроза (172) – диапазон (средняя);

– Угроза (182) – диапазон (высокая);

– Угроза (186) – диапазон (высокая);

– Угроза (186) – диапазон (средняя);

– Угроза (189) – диапазон (высокая);

Общий уровень риска информационной безопасности в компании указывает на то, что показатели риска высоки и угрозы могут быть критичными.

Поэтому, мероприятия, указанные выше, приводят к повешению уровня информационной безопасности.

Хотелось бы добавить, что на современном этапе развития возникает необходимость в дальнейшем совершенствовании существующих методических подходов к оценке информационных рисков хозяйствующих субъектов.

В целях повышения эффективности управления деятельностью предприятия разработана интуитивно понятная и качественная методика оценки информационных рисков хозяйствующего субъекта.

Риски со значением выше 20 подлежат обработке для того, чтобы их минимизировать. После успешного выполнения планируемых организационных мер, в составе методики анализа программного обеспечения технических средств с целью обнаружения возможности возникновения угроз процессам информационной безопасности.

Которые включают в себя следующие меры:

– межсетевое экранирование;

– система резервного копирования, система защиты от НСД;

– система антивирусной защиты;

– учет носителей информации;

– системы видеонаблюдения, адекватные средства физической защиты.

Указанные меры затрагивают аппаратно-программный комплекс и сетевую инфраструктуру, в которых обрабатывается и циркулирует информация, которая имеет ценность.

Остаточный риск становится приемлемым в числовом диапазоне 12.

После обработки рисков остаточный риск стал приемлемым для каждой актуальной угрозы информационной безопасности.

Таким образом, предложенные мероприятия, позволяют оценить риски информационной безопасности на предприятии и требуют минимум финансовых затрат.

Для владельца ценной информацией с точки зрения финансовых потерь, процесс расчета рисков информационной безопасности актуален на всех этапах осуществления мер по защите информации.

Достаточно очевидно, в связи с актуальностью вопроса, необходимость в оценке информационных рисков. Однако практика показывает, что руководство предприятий полностью это не осознает. Для того расставить приоритеты, которые будут определять требования к информационной безопасности и эффективно управлять необходимо оценивать риски.

Как показали результаты отчета мероприятия являются эффективными и повышают уровень защиты. Высокий риск уменьшился в незначительный.

На мой взгляд, необходима адаптированная методика проведения оценки рисков, в условиях нехватка квалифицированных кадров, финансовой ограниченности.

Данный методика оценки, решает указанные проблемы и является адаптивным независимости от размера компании и финансовых возможностей.

В результате проделанной работы можно прийти к выводу:

– проведен анализ сетевой инфраструктуры;

– представлено краткое описание аппаратных ресурсов автоматизированных рабочих мест сотрудников предприятия;

– проведен краткий обзор используемых средств эффективных средств защиты;

– рассмотрены используемые в работе средства предотвращения несанкционированного доступа, мониторинга и предотвращения вторжений;

– представлен список используемых информационных систем предприятия;

– рассмотрены организационные меры безопасности и инженерно-технические решения;

–кратко представлены результаты анализа информационной безопасности;

–описаны рекомендации по организации программно-аппаратных средств обеспечения информационной безопасности;

– представлены рекомендации по организации инженерно-технического комплекса обеспечения информационной безопасности силами предприятия;

–разработана методика анализа программного обеспечения с целью обеспечения возможности возникновения угроз процессам информационной безопасности;

– разработана и протестирована методика рисков и оценка активов.

Глава 3 Обоснование экономической эффективности реализации политики информационной безопасности ООО «Товаротранспортная компания»

3.1 Выбор и обоснование методики расчета экономической эффективности

Экономическая эффективность представляет собой соотношение полученных результатов к произведенным затратам. Существует несколько способов определения экономической эффективности проектов. Методика их применения зависит от ряда факторов:

– тип проекта;

– область применения;

– вид финансового источника.

Рассмотрим теоретические аспекты определения экономической эффективности. Большинство методик расчета экономической эффективности подразделяются на две группы.

Прямой метод определения эффективности. Он основан на расчете экономических показателей до внедрения проекта и после периода его эксплуатации. Прямые методы определения экономической эффективности не всегда удобны в использовании, так как, как правило, для получения финансирования проекта, необходимо определить его экономические показатели раньше, чем он будет внедрен в непосредственную эксплуатацию. Для прямого метода определения экономической эффективности проекта характерны некоторые особенности (независимо от того, какой проект разрабатывается и внедряется). Большинство из них связано корректным определением временного периода оценки эксплуатации проекта. Слишком малый период оценки (месяц, квартал) могут дать некорректные первичные данные, так как на работу предприятия могут играть большое количество факторов:

– конъюнктура рынка;

– сезонный фактор;

– незавершенный цикл бизнес-процессов;

– прочие микроусловия (уровень доходов населения, возраст клиентов).

В то же время слишком большой период (1 год, 3 года, 5 лет) оценки требует долговременных наблюдений и также способен приводить к искажениям в расчетах экономической эффективности внедрения проекта. Одним из долгосрочных факторов является оценка дисконтирования денежных потоков.

Дисконтирование денежных потоков можно представить, как расчет ожидаемых экономических эффектов в пересчете на текущий момент. В силу ряда негативных факторов (основные из них – инфляция, финансовые риски, кредитное обслуживание) стоимость затрат будущих периодов нелинейно возрастает и долгосрочные проекты (а также долгосрочное наблюдение за проектами) приводит к возрастанию как прямых, так и косвенных расходов. Поэтому база следующего периода оценки нелинейно увеличивается по отношению к расчетной базе прошлого периода. Весь период разбивается на одинаковые промежутки времени (как правило, месяц, реже квартал), каждый последующий период рассчитывается с опорой на прошлый период и поправочный коэффициент (дисконт).

Косвенный метод расчета определения эффективности. Данный вид методов расчета применяется там, где получение прямых показателей эффективности затрудненно или не представляется возможным. Эффективность выражается либо непосредственно в количественных отчетных показателях деятельности (количество клиентов, время обслуживания одного клиента), либо в их условных денежных эквивалентах (стоимость часа работы - специалиста).

Большую роль играют синергетические эффекты (как положительные, так и отрицательные), проявление которых возможно в различных сферах:

– изменение морального климата в коллективе;

– изменение качества оказываемых услуг;

– изменение отношения клиентов к обслуживанию;

– снижение (повышение) энергозатрат;

– изменение скорости работы сотрудников в информационных системах обработки персональных данных;

– изменение времени регламентных процедур.

В большинстве случаев плановое определение синергетических эффектов невозможно (что является частым явлением при внедрении информационных проектов), так как большинство проводимых работ в сфере повышения информационной безопасности предприятия являются адресными и индивидуальными, в зависимости от:

– уровня квалификации персонала;

– текущего состояния информационной защиты в учреждении;

– рекомендуемых мер по повышению информационной безопасности.

Для оценки прямых затрат информационных проектов используется анализ экономической эффективности на основе сравнения показателей с предыдущим периодом (до реализации проекта), формула 2.

$$З_{Δ} = З_{иб0} - (З_{пр} + З_{иб1}) \quad (2)$$

где $З_{Δ}$ – изменение затрат;

– $З_{иб0}$ – затраты на защиту информации до внедрения проекта;

– $З_{пр}$ – затраты на реализацию проекта по повышению мер информационной защиты;

– $З_{иб1}$ – затраты на защиту информации после внедрения проекта.

Затраты на информационную безопасность являются динамическим показателем, поэтому их следует брать в одном временном диапазоне (месяц, квартал, год). Следует учитывать, что большие временные интервалы будут приводить к искажениям, так как необходимо учитывать дисконтирование денежных потоков. Кроме того, расчет изменения затрат возможен после

истечения контрольного срока измерения $З_{иб1}$.

Состав затрат на реализацию проекта по повышению мер информационной защиты представлен ниже, формула (3):

$$З_{пр} = ФОТ + З_{м} + З_{усл} + Р_{н}, \quad (3)$$

где ФОТ – фонд оплаты труда;

– $З_{м}$ – материальные затраты;

– $З_{усл}$ – затраты, связанные с работами и услугами;

– $Р_{н}$ – накладные расходы.

Фонд оплаты труда представляет собой совокупность всех расходов проекта, связанные с оплатой труда, формула (4):

$$ФОТ = Зар + О_{ПФР} + О_{ФСС} + О_{ФОМС}, \quad (4)$$

где Зар – заработная плата участников проекта;

– $О_{ПФР}$ – отчисления в ПФР (22% от начисленной заработной платы);

– $О_{ФСС}$ – отчисления в Фонд социального страхования (2,9% от начисленной заработной платы);

– $О_{ФОМС}$ – отчисления в Фонд обязательного медицинского страхования (5,1% от начисленной заработной платы).

Следует отметить, что в структуре заработной платы (Зар) следует выделять также НДФЛ (13% из заработной платы, при условии отсутствии льгот).

Материальные затраты ($З_{м}$) представляют совокупность всех затрат, связанных с приобретением полуфабрикатов, расходных материалов, запасных частей и оборудования.

Затраты, связанные с работами и услугами ($З_{усл}$) содержат следующие элементы:

– коммунальные услуги (если они были необходимы во время

выполнения проекта);

– услуги связи;

– услуги подрядных организаций;

– работы по выполнению государственной экспертизы (если она необходима для выполнения проекта);

– почтовые расходы;

– доставка узлов, машин и агрегатов;

– приобретение неисключительных лицензионных прав на использование программного обеспечения;

– услуги обязательного технического сопровождения специализированного программного обеспечения и оборудования;

– прочие услуги ресурсоснабжающих организаций (например, выполнение электромонтажных работ компанией, выполняющий обслуживание электрических сетей).

Накладные расходы ($Р_н$) представляют собой дополнительный поправочный коэффициент, связанный с возникновением дополнительных непредвиденных расходов и платежей (пошлины, аренда помещения, реклама, информационные и консультационные услуги и т.д.). Особенность накладных расходов – сложность их точного планирования, часть расходов могут возникать в одном проекте, и не появляться в другом. Поэтому накладные расходы учитываются единым поправочным коэффициентом от 10 до 30% от всех остальных затрат. Специфика накладных расходов в информационных проектах определяет его коэффициент в 10-15%.

Таким образом, произведен выбор и обоснование методики расчета.

3.2 Расчет показателей экономической эффективности проекта

Перед непосредственным расчетом затрат на выполнение предложенных мер необходимо рассмотреть краткую характеристику предлагаемого программного обеспечения и оборудования.

Сетевое оборудование. Поскольку сетевой шлюз, используемый на предприятии, отвечает требованиям информационной безопасности, выполнять его смену нет необходимости. В то же время в целях оптимизации и усовершенствовании сетевой инфраструктуры, формирования резерва портов для дальнейшего расширения локальной сети предприятия требуется замена коммутатора D-Link DES-1005D/E.

Требования к оборудованию:

– количество портов – не менее 16, для уменьшения количества агрегирующих коммутаторов и сокращения нагрузки на локальную сеть предприятия;

– стоимость оборудования – из рассматриваемого спектра доступного на рынке оборудования предлагается выбирать наименьший по цене при прочих равных характеристиках.

Для защиты сетевого оборудования необходимо использование телекоммуникационных шкафов. Телекоммуникационный шкаф представляет собой специальную закрытую конструкцию для установки сетевого и телекоммуникационного оборудования. Телекоммуникационные шкафы выполняют из листового металла с дверцами, запираемыми на ключ, они имеют специальные стандартизированные крепления для установки промышленного сетевого оборудования.

Основные требования к телекоммуникационным шкафам:

– Габариты – очень часто при проектировании зданий и помещений, их использование не учитывается и место для их установки, как правило, необорудованное. Поэтому габариты и конструктивное исполнение коммуникационных шкафов имеет большую роль.

– Тип исполнения – напольный или настенный. Имеются универсальные модели, имеющие крепления как для установки на пол, так и для монтажа на стены помещения.

– Место установки – уличные шкафы и шкафы для помещений.

– Тип комплектации – сборные и разборные. Разборные поставляются в

виде отдельных компонентов, требуется их сборка и монтаж. Сборные поставляются в готовом к эксплуатации виде.

– Устанавливаемое оборудование – стандартное, регулируемое.

В продаже отсутствуют специальные металлические шкафы для хранения машинных носителей. Вместо них допускается применять любой запираемый металлический шкаф (для хранения офисных документов) или сейф. Сейфы не рассматриваются для использования в проекте в виду их высокой стоимости, кроме того, в шкафу возможно хранение документации, связанной с защитой информации и обработкой персональных данных.

Автоматизированные рабочие места сотрудников. Парк имеющегося оборудования (Dell Wyse – 100 шт., Intel NUC – 20 шт., Kraftway – 30 шт.) морально устарел и не может решать имеющиеся задачи своевременно и в полном объеме. Поэтому предлагается их полная замена (в несколько этапов, чтобы не нарушать бизнес-процессы предприятия).

Требования к оборудованию:

– процессор – Intel Core i5 10400 (или большей производительности);

– количество ядер процессора – 6 шт;

– оперативная память – 8 Гб, DDR4;

– накопители памяти – SSD, объем не менее 256 Гб;

– операционная система – Windows 10 в комплекте поставки;

– форм-фактор – Slim;

– наименьшая цена, при прочих равных условиях.

Проведем расчеты в соответствии с предложенной методикой, рассчитаем затраты на выполнение проекта ($З_{пр}$). Для реализации проекта не требуется привлечение стороннего персонала, так как в учреждении имеется штатная единица администратора информационной безопасности. Соответственно выделять специальный фонд оплаты труда нет необходимости, ФОТ=0.

Материальные затраты $З_{м}$:

– коммутаторы TP-Link TL-SG116 16G – 2 шт. (на замену D-Link DES-

1005D/E), цена – 3590,00 рублей;

– шкаф телекоммуникационный ITK LWE3-09U53-GF – 3 шт. (дополнительный для сетевого шлюза), ориентировочная цена – 2800,00 рублей;

– запираемый металлический шкаф для хранения машинных носителей информации ШХА-50 (40)/670 – 1 шт., ориентировочная цена 3773,30 рублей.

– системный блок Lenovo IdeaCentre 3 07IMB93 – 150 шт., ориентировочная цена – 39999,00 руб.

$$З_м = 3590{,}00 \times 2 + 2800{,}00 \times 3 + 3773{,}30 + 150 \times 39999{,}00$$
$$= 6019203{,}30 \text{ руб.}$$

Затраты, связанные с работами и услугами ($З_{усл}$).

Антивирусное программное обеспечение.

Требования:

– защита автоматизированных рабочих мест сотрудников;

– своевременное обновление антивирусных баз;

– программное обеспечение российских разработчиков;

– предоставление комплексной защиты (антивирусное программное обеспечение, защита от внешних вторжений, брандмауэр);

– наименьшая цена, при прочих равных условиях.

– Dr. Web Security Space, лицензия на 1 год – 800 руб. (при условии приобретения не менее 100 лицензий);

– Kaspersky Endpoint Security, на 1 год – 1200,00 руб. (при условии приобретения не менее 50 лицензий).

Для реализации в проекте был выбран Kaspersky Endpoint Security.

Средство резервного копирования. Представляет собой сервисное программное обеспечение, назначение которого создание копий папок и файлов на отдельный носитель. Использование резервных копий данных позволяет провести восстановление в случае аппаратных сбоев и намеренных

деструктивных действий.

Требования к средству резервного копирования:

– доступ по логину и паролю;

– копирование по расписанию;

– десктопное приложение или приложение командной строки;

– бессрочная лицензия;

– наименьшая цена, при прочих равных условиях.

Список рассматриваемых программ:

- Effector saver – 3500,00 руб.;
- Paragon Protect & Restore Server – 3725,00 руб.;
- Macrium Reflect 7 Workstation – 3450,00 руб.;
- Macrium CMC Starter Pack – 1200,00 руб., за одну лицензию при условии приобретения 15 лицензий;
- AOMEI Backupper –1350,00 руб., за одну лицензию при условии приобретения 10 лицензий;
- Veeam Disaster Recovery Orchestrator – 3136,00 руб.;
- Acronis Защита - Данных Расширенная для платформы виртуализации – 4729,00 руб.;
- Veritas System recovery desktop ed – 5887,00 руб.;
- Elcomsoft System Recovery – 5995,00 руб.;
- EasyRecovery – 7087,00 руб.;
- Hetman Data Recovery Pack – 5400,00 руб.;
- Handy Backup workstation – 1000,00 руб., лицензия на 3 года.

Выбрано средство резервного копирования Veeam Disaster Recovery Orchestrator.

$$З_{усл} = 800{,}00 \times 150 + 3136{,}00 = 123136{,}00 \text{ руб.}$$

Накладные расходы ($Р_н$), используем коэффициент 15%:

$$Р_н = (0{,}00 + 6019203{,}30 + 123136{,}00) \times 13\% = 798504{,}11 \text{ руб.}$$

Всего затрат на реализацию проекта:

$$З_{пр} = 0{,}00 + 6019203{,}30 + 123136{,}00 + 798504{,}11 = 6940843{,}41 \text{ руб.}$$

Структура затрат (рисунок 17) показана на диаграмме.

Рисунок 17 – Структура затрат

Проведем сравнение затрат, использованных средств защиты с затратами на проект изменения информационной безопасности. Затраты на использованные средств информационной защиты представлены в таблице 4.

Таблица 4 – Затраты на информационную безопасность предприятия

Наименование	Кол-во	Цена	Стоимость
SecretNet Studio	37	6764,00	250268,00
Scaner-VS-08	1	10000,00	10000,00
VipNet Custom	37	8177,00	302549,00

Итого, затрат на содержание систем информационной безопасности: 562817,00 руб.

Теперь необходимо рассмотреть, совокупные затраты при внедрении проекта. Более подробном можно рассмотреть в таблице 5.

Таблица 5 – Совокупные затраты при внедрении проекта

Наименование	Кол-во	Цена	Стоимость
SecretNet Studio	37	6764,00	250268,00
Scaner-VS-08	1	10000,00	1000,00
VipNet Custom	37	8177,00	302549,00
Коммутатор TP-Link TL-SG116 16G	2	3590,00	7180,00
Шкаф телекоммуникационный ITK LWE3-09U53-GF	3	2800,00	8400,00
Шкаф ШХА-50 (40)/670	1	3773,30	3773,30
Kaspersky Endpoint Security	150	1200,00	180000,00
Veeam Disaster Recovery Orchestrator	1	3136,00	3136,00
Накладные расходы	-	-	798504,11
Системный блок Lenovo IdeaCentre 3 07IMB93	150	39999,00	5999850,00

Итого, затрат после внедрения проекта: 7554660,41 руб.

Затраты в относительном выражении составили:

7554660,41 / 562817,00 × 100 = 1342 %

Приведем оценку динамики величин потерь за три квартала рассмотрено в таблице 6. Данные таблицы показывают положительный эффект от совершенствования информационной безопасности на предприятии ООО «Товаротранспортная компания».

Таблица 6 - Оценка динамики величин потерь

Показатели	1 кв.	2 кв.	3 кв.
До внедрения проекта на предприятии	80	160	340
После внедрения проекта на предприятии	58	60	110
Снижение потерь	22	100	230

Экономические расчеты показывают эффективность внедрения комплекса информационной защиты на предприятие ООО «Товаротранспортная компания».

Итак, можно прийти к выводу, что управление информационной безопасностью важная часть менеджмента всего предприятия, обеспечивающая эффективность различных процессов и решающая не только тактические, но и стратегические задачи по защите ценной информации.

В ходе исследования обнаружилась необходимость рассчитать и показать экономическую эффективность. Указанные выше мероприятия, позволяют реализовать подход совершенствования управления информационной безопасности на предприятии.

Применив приводнённые мероприятия на основе политики информационной безопасности на практике в ООО «Товаротранспортная компания», можно сделать вывод, что указанные мероприятия повышают уровень информационной безопасности.

В данной главе, была выбрана методика расчета затрат на реализацию проекта по внедрению актуальным мероприятий для предприятия. Определены основные статьи затрат, их фактическая величина и конечная сумма. Для планирования бюджета предприятия, в части выполнения требований по информационной безопасности. В результате на выполнение предложенных рекомендаций по повышению мер информационной безопасности требуется 7554660,41 руб.

Для планирования своего бюджета хозяйствующему субъекту, необходимо знать, затраты на обеспечение информационной безопасности.

Так как, это не маловажно для расстановки приоритетов при управлении бизнес-процессов.

Заключение

Подводя итоги, можно сделать вывод о том, в ходе выполнения работы разработаны решения проблем при построении процесса управления безопасностью для защиты ценных информационных ресурсов.

Управление информационной безопасностью тесно связанна с непрерывности бизнес-процессов. Не принимая эффективных мер и политики по управлению информационной безопасности чревато остановкой непрерывности бизнес-процесса.

В ходе исследования обнаружилась существенная проблема. Это дискретность при управлении процессами информационной безопасностью.

Информационная безопасность — это всесторонняя защищённость информации и поддерживающей её инфраструктуры от любых случайных или злонамеренных воздействий.

Основной целью управления информационной безопасностью является поддержание информационных ресурсов в соответствии с заданными требованиями. Для достижения этой цели управление должно быть построено таким образом, чтобы минимизировать время и ресурсы, направляемые на управление информационными ресурсами. Решить данную проблему, способна грамотно созданная политика информационной безопасности.

В процессе выполнения работы был проведен анализ средств информационной безопасности и информационной инфраструктуры предприятия ООО «Товаротранспортная компания». Указаны недостатки и представлены мероприятия по повышению уровня информационной безопасности, через технические средства в которых проходят информационные потоки.

В ходе изучения, была представлена методика и результаты анализа программного обеспечения технического средства с целью обнаружения возможности возникновения угроз процессам информационной безопасности.

В ходе анализа были представлены UML– диаграммы:

– UML – диаграмма последовательности действий, выполняемых в процессе сборки и развертывания программного обеспечения;

– UML– диаграмма последовательности действий анализа программного обеспечения технического средства;

– UML – диаграмма последовательности действий при восстановлении алгоритма ПО.

В результате предоставил обоснование экономической эффективности реализации системы в составе политики информационной безопасности.

Проанализировав, можно сделать вывод о том, обосновывая вероятность отказов (сбоев) технического средства и программного обеспечения, обнаруживается актуальная проблема при управлении процесса информационной безопасности в корпоративной информационной системе. Реализована модернизация управления информационной безопасности на предприятии ООО «Товаротранспортная компания». Представлены мероприятия по совершенствованию информационной безопасности. Разработана адаптивная методика анализа программного обеспечения технических для хозяйствующих субъектов независимо от их финансовых возможностей.

Произведённый анализ оценки рисков для минимизации потерь, показал целесообразность внедрения мероприятий на предприятии. Высокий риск уменьшился в незначительный.

Произведены расчеты экономической эффективности реализации политики информационной безопасности в ООО «Товаротранспортная компания». Высокий риск уменьшился в незначительный.

В заключение хотелось бы подчеркнуть, что указанные мероприятия и методика, не исключают каких–либо недостатков, в связи с этим необходимо дальнейшее исследование. Учитывая, что все поставленные задачи решены, можно утверждать, что главная цель исследования – достигнута.

Список используемой литературы и источников

1. Баранова, Е.К. Информационная безопасность. История специальных методов криптографической деятельности: Учебное пособие / Е.К. Баранова, А.В. Бабаш, Д.А. Ларин. - М.: Риор, 2018. - 400 с.
2. Бегишев, И.Р. Безопасность критической информационной инфраструктуры Российской Федерации / И.Р. Бегишев // Безопасность бизнеса. - 2019. - № 1. - С. 27-32.
3. Бегишев И.Р. Уголовная ответственность за приобретение или сбыт цифровой и документированной информации, заведомо добытой преступным путем / И.Р. Бегишев // Актуальные проблемы экономики и права. - 2018. - № 1. - С. 123-126.
4. Бегишев И.Р. Современное состояние преступлений в сфере обращения цифровой информации/ И.Р. Бегишев // Информация и безопасность. - 2017. - № 4. - С. 567-572.
5. Бегишев И.Р. Синдром безопасной атаки: юридико-психологический феномен / И.Р. Бегишев // Юридическая психология. - 2018. - № 2. - С. 27-30.
6. Бегишев И.Р. Создание, использование и распространение вредоносных компьютерных программ/ И.Р. Бегишев // Проблемы права. - 2017. - № 3. - С. 218-221.
7. Бирюков, А.А. Информационная безопасность: защита и нападение / А.А. Бирюков. - М.: ДМК Пресс, 2017. - 474 с.
8. Гафнер, В.В. Информационная безопасность: Учебное пособие / В.В. Гафнер. - Рн/Д: Феникс, 2018. - 324 с.
9. Герасименко, В.А. Основы защиты информации : учеб. пособие. / В.А. Герасименко., А.А. Малюк -М. : МГИФИ, 2018. - 538 с.
10. Грибунин, В.Г. Комплексная система защиты информации на предприятии : учебное пособие для вузов / В.Г. Грибунин, В.В. Чудовский. - М. : Академия, 2019. - 416 с.

11. Гришина, Н.В. Информационная безопасность предприятия: Учебное пособие / Н.В. Гришина. - М.: Форум, 2018. - 118 с.

12. Громов, Ю.Ю. Информационная безопасность и защита информации: Учебное пособие / Ю.Ю. Громов, В.О. Драчев, О.Г. Иванова. – М.: ТНТ, 2017. - 384 с.

13. Диева, С.А. Организация и современные методы защиты информации / С.А. Диева - М. : Концерн «Банковский деловой центр, 2018. - 472с.

14. Зайцев, А.П. Техническая защита информации : учебник для вузов / А.П. Зайцев, А.А. Шелупанов. - М. : Горячая линия - Телеком, 2017. - 616 с.

15. Запечников, С.В. Информационная безопасность открытых систем. Том 1. Угрозы, уязвимости, атаки и подходы к защите: Учебник для вузов. / С.В. Запечников, Н.Г. Милославская, А.И. Толстой, Д.В. Ушаков. - М.: ГЛТ , 2016. - 536 с.

16. Керимов В.Э. Профилактика и предупреждение преступлений в сфере компьютерной информации /В.Э. Керимов // "Черные дыры" в Российском законодательстве. - 2017. - № 1. - С.43

17. Краковский, Ю.М. Информационная безопасность и защита информации : учеб.пособие/ Ю. М. Краковский. - М. ; Ростов н/Д : МарТ, 2018. - 287 с.

18. Ловцов Д. А. Проблема гарантированного обеспечения информационной безопасности крупномасштабных автоматизированных систем // Правовая информатика. 2017. - № 3. - С. 66—74.

19. Малюк, А.А. Информационная безопасность: концептуальные и методологические основы защиты информации / А.А. Малюк. - М.: ГЛТ, 2017. - 280 с.

20. Партыка, Т.Л. Информационная безопасность: Учебное пособие / Т.Л. Партыка, И.И. Попов. - М.: Форум, 2018. - 88 с.

21. Петренко С.А. Оценка затрат на защиту информации / С.А. Петренко//Защита информации. - 2017. - № 1. – С.56

22. Петраков, А.В. Основы практической защиты информации : учебное пособие для вузов / А.В. Петраков - М. : Радио и связь, 2017. - 203 с.

23. Петров, С.В. Информационная безопасность: Учебное пособие / С.В. Петров, И.П. Слинькова, В.В. Гафнер. - М.: АРТА, 2016. - 296 с.

24. Рыженкова О. Ю. Информационная безопасность: определение понятия, местов системе национальной безопасности // Закон и право. - 2017. - № 1. - с. 50 - 52.

25. Семененко, В.А. Информационная безопасность / В.А. Семененко. - М.: МГИУ, 2018. - 277 с.

26. Сидорин, Ю.С. Технические средства защиты информации: учеб. пособие / Ю.С. Сидорин - СПб. : Изд-во Политехн. ун-та, 2012. - 141 с.

27. Смирнова, А.Н. Защита информации : учебник для вузов / А.Н. Смирнова. - М. : Смарт, 2017. - 176 с.

28. Стрельцов, А.А. Обеспечение информационной безопасности России / Под ред. В.А. Садовничего и В.П. Шерстюка - М. : МЦНМО, 2017. - 296 с.

29. Тедеев, А.А. Информационное право : учебник для вузов / А.А. Тедеев - М. : Эксмо, 2018. - 464 с.

30. Тимец, Б.В. Сделайте свой офис безопасней : учебник для вузов / Б.В. Тимец. - М. : Конфидент, 2019. - 100 с.

31. Титоренко, Г.А. Информационные технологии управления : учеб. пособие для вузов / Г. А. Титоренко. - М. : ЮНИТИ-ДАНА, 2017. - 439 с.

32. Торокин, А.А. Основы инженерно - технической защиты информации : учебник для вузов / А.А. Торокин. - М. : Ось, 2018. - 336 с.

33. Чипига, А.Ф. Информационная безопасность автоматизированных систем / А.Ф. Чипига. - М.: Гелиос АРВ, 2018. - 336 с.

34. Шаньгин, В.Ф. Информационная безопасность и защита информации / В.Ф. Шаньгин. - М.: ДМК, 2017. - 702 с.

35. Шаньгин, В.Ф. Информационная безопасность компьютерных систем и сетей: Учебное пособие / В.Ф. Шаньгин. - М.: Форум, 2018. - 256 с.

36. Шаньгин, В.Ф. Защита компьютерной информации. Эффективные методы и средства. М.: ДМК Пресс, 2019. - 458 с.

37. Шрамков, И.Г. Защита и обработка конфиденциальных документов : учеб. пособие / И.Г. Шрамков, Ю.Г. Крат. - Хабаровск : Изд-во ДВГУПС, 2017. - 500 с.

38. Электронная версия журнала InfoWatch [Электронный ресурс] // Режим доступа: URL: https://www.infowatch.ru/sites/default/files/analytics/files/InfoWatch_%D0%9C%D0%B8%D1%80_%D0%A3%D1%82%D0%B5%D1%87%D0%BA%D0%B8_2020_v.1.17.pdf

39. Ярочкин, В.И. Технические каналы утечки информации : учебник для вузов / В.И. Ярочкин. - М. : ИПКИР, 2018. - 106 с.

40. Ярочкин, В.И. Система безопасности фирмы : учебник для вузов / В.И. Ярочкин. - М. : Ось-89, 2018. - 192 с.

41. Authors: T. Rama Reddy, P. V. G. D. Prasad Reddy, Rayudu Srinivas, Ch. V. Raghavendran, R. V. S. Lalitha and B. Annapurna. Citation: EURASIP Journal on Information Security 2021 2021:7. Content type: Research. Published on: 26 Jun. 2021.

42. Haleplidis E., "Software-defined networking (SDN): Layers and architecture terminology", Inc., Released Jun. 2017.

43. Sonia Burney, Sabrina Burney. "Security and Frontend Performance .O'Reilly Media", Inc., Released Jan. 2017/ Publisher(s): O'Reilly Media, Inc. ISBN: 9781491972151.

44. Veitch P., Curley E., Kantecki T. "Performance Evaluation of Cache Allocation Technology for NFV Noisy Neighbor Mitigation" // 2017 IEEE Conference on Network Softwarization (NetSoft), 3-7 July 2017, Bologna, Italy.

45. Yan Q. et al. "Software-defined networking (SDN) and distributed denial of service (DDoS) attacks in cloud computing environments" // IEEE communications surveys & tutorials. - 2017. - Т. 18. - №. 1. - С. 602-622.