МИНИСТЕРСТВО ОБРАЗОВАНИЯ И НАУКИ РОССИЙСКОЙ ФЕДЕРАЦИИ

федеральное государственное бюджетное образовательное учреждение
высшего образования
«Тольяттинский государственный университет»

ИНСТИТУТ МАТЕМАТИКИ, ФИЗИКИ И ИНФОРМАЦИОННЫХ ТЕХНОЛОГИЙ

Кафедра «Прикладная математика и информатика»

09.03.03 Прикладная информатика

Бизнес-информатика

БАКАЛАВРСКАЯ РАБОТА

на тему: Разработка политики информационной безопасности предприятия (на примере ООО Саунбилд)

Студент Николай Валерьевич Куликов _____

Руководитель Оксана Михайловна Гущина _____

Заведующий кафедрой к.тех.н., доцент, А.В. Очеповский _____

«_____»_____20_____г.

Тольятти 2017

АННОТАЦИЯ

С. 76, рис. 11, табл. 15, лит. 37 источников

ЦЕЛЬ ЗАЩИТЫ ИНФОРМАЦИИ, ЗАЩИТА ИНФОРМАЦИИ ОТ УТЕЧЕК, ПОЛИТИКА ИНФОРМАЦИОННОЙ БЕЗОПАСНОСТИ, ИНФОРМАЦИОННАЯ БЕЗОПАСНОСТЬ, ISO 27001, ISO 27002.

Разработана политика информационной безопасности предприятия общества с ограниченной ответственностью "Саунбилд".

Проведен анализ системы данных ООО "Саунбилд", приведены технико-экономические характеристики, выявлены основные проблемы и задачи защиты информации. Произведен сравнительный анализ методов и средств защиты информации в строительной организации. Произведен выбор и обоснование методов зашиты информации в корпоративной сети строительной организации. Разработана политика информационной безопасности строительной организации, предлагающая средства и методы защиты данных.

Произведен расчет эффективности от реализации рекомендаций по повышению уровня информационной безопасности.

Работа находится на стадии рассмотрения руководством компании предложенной концепции по улучшению информационной защиты данных и принятию политики информационной безопасности.

ОГЛАВЛЕНИЕ

ВВЕДЕНИЕ

Появление новых информационных технологий и развитие мощных компьютерных систем хранения и обработки информации повысили требования к уровню защиты информации и определили необходимость разработки эффективных механизмов защиты информации, адаптированной под современные архитектуры хранения данных. Так постепенно защита экономической информации становится обязательной: разрабатываются всевозможные документы по защите информации; формируются рекомендации по защите информации; приводится Федеральный закон о защите информации, который рассматривает проблемы защиты информации и задачи защиты информации, а также решает некоторые уникальные вопросы защиты информации.

Обеспечение защиты информации в компании является непрерывным процессом, который предусматривает применение современных методов, позволяющих вести контроль внешней и внутренней среды предприятия, организацию и реализацию мероприятий по поддержке стабильного функционирования локальной сети и вычислительной техники, а также минимизацию потерь в связи с утечкой информации. Для осуществления защиты информации, как в сетях, так и на производстве, на предприятиях должен быть сформирован определенный свод правил и нормативных документов, регламентирующих действия сотрудников по обеспечению безопасности и описывающий технические и программные средства для защиты информации. Данный свод документов называется политикой информационной безопасности.

Политика информационной безопасности направлена на минимизацию рисков утечки информации на предприятии, а также для устойчивого функционирования информационной структуры предприятия. Это может привести к финансовым потерям в связи с утечкой информации, поэтому необходимо уделять пристальное внимание вопросам информационной безопасности.

Таким образом, угроза защиты информации сделала средства обеспечения информационной безопасности одной из обязательных характеристик информационной политики любой компании. Другими словами, вопросы защиты информации решаются для того, чтобы изолировать нормально функционирующую информационную систему от несанкционированных управляющих воздействий и доступа посторонних лиц или программ к данным с целью хищения.

Объектом исследования ВКР являются методы и средства защиты данных предприятия ООО "Саунбилд", а **предметом исследования** – организация политики информационной безопасности ООО "Саунбилд".

Цель ВКР: разработка политики информационной безопасности предприятия, а также методов и средств, позволяющих повысить защиту информации в ООО "Саунбилд".

Для достижения обозначенной цели необходимо решить следующие задачи:

1. Оценить текущее состояние информационной безопасности предприятия.
2. Выявить нарушения в защите информационной безопасности, а также выявление наиболее вероятных угроз информации.
3. Рассмотреть основные проблемы, задачи и принципы защиты информации.
4. Произвести анализ и классификацию угроз, уязвимых мест в компьютерных сетях компании.
5. Разработаны предложения по реализации административных, программно-аппаратных и инженерно-технических мер по предотвращению угроз информационной безопасности.
6. Оценить эффективность разработанного комплекса, направленного на организацию политики информационной безопасности строительной организации.

Практическая значимость работы заключается в том, что предложенная модель политики информационной безопасности может быть использована в практике действующих предприятий.

При написании ВКР использовались научные труды следующих авторов: Аверченкова В. И. [1], Алексанова А. К. [2], Анина Б. Ю. [3], Башлы П. Н. [5], Беленькой М.Н. [6], Бурняшова Б.А. [8], Герасименко В. А. [9], Зайцева А. П. [12], Мельникова В. В. [20], Осипова В. Ю. [21], Партыки Т.Л. [22], Романова С. К. [23], Садердинова А. А. [25] и других.

Выпускная квалификационная работа состоит из: Введения, трех основных глав, Заключения, Списка использованной литературы.

В первой главе произведен анализ системы защиты данных в строительной компании

Во второй главе произведена разработка политики информационной безопасности

В третьей главе рассмотрено обоснование экономической эффективности реализации политики информационной безопасности строительной организации

Глава 1 АНАЛИЗ СИСТЕМЫ ЗАЩИТЫ ДАННЫХ В СТРОИТЕЛЬНОЙ КОМПАНИИ

1.1 Технико-экономическая характеристика строительной компании

Компания ООО «Саунбилд» предлагает весь комплекс общестроительных работ - от создания проектной документации до выполнения чистовых отделочных работ и комплектации объектов материалами по оптовым ценам. Деятельность фирмы сконцентрирована на полном обеспечении процесса строительства саун, бань, бассейнов, турецких бань и т.д. от выбора проекта и заканчивая сдачей реализованного строительного объекта «под ключ». Сочетание кратчайших сроков выполнения заказов и приемлемых цен, применение современных материалов и соблюдение высокого качества делают фирму ООО «Саунбилд» достаточно конкурентоспособной в сфере строительства.

Строительная фирма ООО «Саунбилд» имеет значительный опыт в монтаже и проведении работ по устройству инженерных систем и оборудования, использует в работе современные передовые технологии и оборудование. Рабочие бригады, занимающиеся монтажом, имеют высокую квалификацию и солидный опыт, которые позволяют выполнять заказы в кратчайшие сроки без лишних задержек, а также прокладывать инженерные системы в местах, к которым достаточно сложно обеспечить нормальный доступ. Опытные сотрудники фирмы проводят качественные консультации по монтажу, замене или модернизации инженерных сетей, а также рассказывают о новых тенденциях в развитии инженерных систем, о наиболее оптимальных, качественных и экономичных решениях задач, которые необходимо реализовать.

Строительная фирма ООО «Саунбилд», занимающаяся работами по устройству инженерных систем и оборудования, обеспечивает комплексный подход к выполнению поставленных целей, начиная от исследования и анализа объектов, сбора данных и проведения необходимых замеров, составления

проектно-сметной документации и заканчивая устройством, монтажом и эксплуатационным тестированием инженерных систем.

В таблице 1.1 приведены общие технические характеристики предприятия.

Таблица1.1 - Характеристика предприятия

№ п\п	Наименование характеристики (показателя)	Значение показателя на определённую дату либо за период	Единицы измерения
1	Годовой оборот	160 562 000	руб.
2	Балансовая стоимость предприятия	86 586 000 руб.	руб.
3	Годовой фонд заработной платы	78 000 000 руб.	руб.
4	Количество работников	34	чел.
5	Количество партнёров предприятия	Более 50 фирм	Шт.
6	Рентабельность предприятия	Не менее 16%	

К основным направлениям деятельности ООО «Саунбилд» относятся:

- строительство зданий и сооружений;
- производство отделочных работ;
- подготовка строительного участка;
- монтаж инженерного оборудования, зданий и сооружений;
- производство столярных, плотничных, малярных и стекольных работ;
- устройство покрытий полов и облицовки стен;
- производство прочих строительных работ.

Миссией ООО «Саунбилд» является развитие деятельности компании за счет высокого качества выполнения строительных работ, оптимальной ценовой политики и новейших технологий.

Для поддержки своего имиджа компанией выполняются следующие задачи:

- устанавливаются единые критерии поддержки имиджа среди работников компании, бизнес-среде, с органами государственной власти и общественными организациями;
- формируется и поддерживается среда взаимного уважения, открытости и доверия с гарантией защиты их прав;
- укрепляется имидж компании за счет репутации эффективного, социально ответственного и надежного партнера.

Для поддержки имиджа у работников, приоритетами компании являются жизнь и здоровье, поддержка социальной обеспеченности и постоянное повышение профессионализма сотрудников.

Структура управления предприятием построена по иерархическому принципу и изображена на рис. 1.1.

Рисунок 1.1 – Организационная структура компании «Саунбилд»

Строительная фирма ООО «Саунбилд», состоящая из множества структурных подразделений, предоставляет всем отделам в равной степени доступ ко всем данным, находящимся в базе данных (БД), что приводит к

неправильной работе самой БД, а также возможности предоставления закрытой информации лицам, у которых не должно быть доступа, т.е. к неправильной организацией политики информационной безопасности. Соответственно можно сделать вывод, что данная схема организации доступа к данным имеет большое количество потенциальных угроз информационной безопасности и для улучшения защиты данных необходимо разграничить доступ в данную систему. На рис. 1.2 представлена схема обработки заявки от клиента.

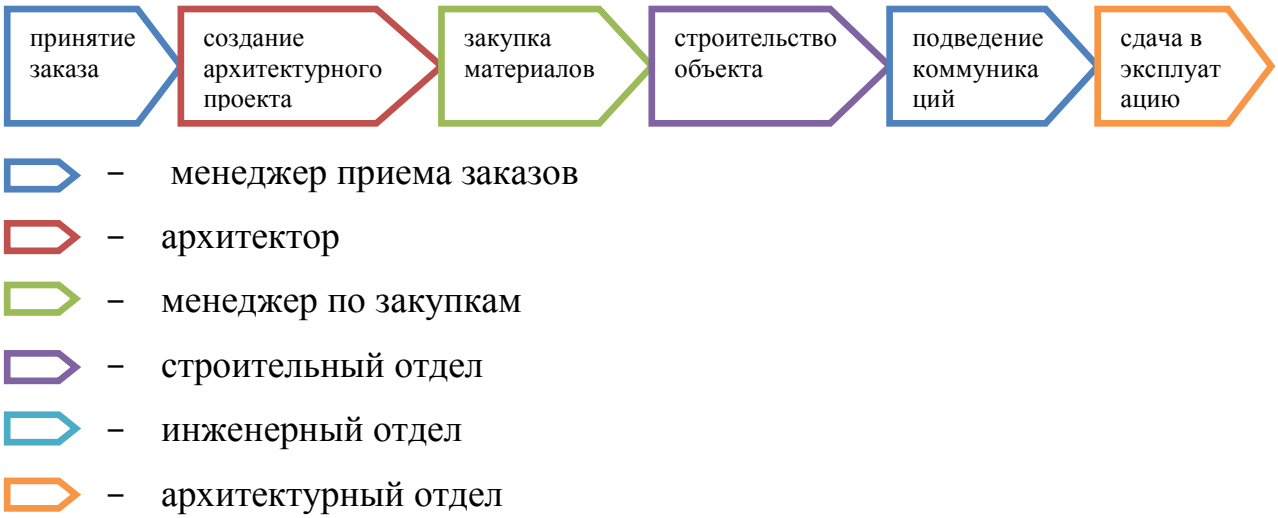


Рисунок 1.2 – Структурная схема обработки заявки от клиента

Из рисунка 1.2 мы можем видеть, что информация от принятия заказа от клиента и до сдачи в эксплуатацию происходит общим потоком и для всех одинакова. Что подтверждает фактор угрозы информационной безопасности.

Для более детального понимания системы организации информационной безопасности в компании считаю необходимым рассмотреть основные активы, использующиеся в организации для обоснования необходимости защиты информации.

1.2 Анализ и оценка защиты данных в активах строительной организации

Изучение сферы деятельности организации позволило выявить следующие информационные активы:

- информация/данные (в т.ч. секретная документация генпланов городских коммуникаций, проектная документация организаций, личные данные клиентов и т.д.);
- аппаратные средства (компьютеры, хранилища данных, оргтехника);
- программное обеспечение, включая прикладные программы (в т.ч. средства САПР);
- документы в бумажном виде (в т.ч. договора, сканы генпланов, выписки из государственных реестров и т.д.);
- конфиденциальность и доверие при оказании услуг.

Все активы компании можно рассмотреть с позиции ценности и расположить их в порядке возрастания:

- прикладное программное обеспечение (в т.ч. САПР, CMS, ERP, CRM и т.д.);
- системное программное обеспечение;
- личные сведения о сотрудниках;
- Личные данные клиента;
- проектная документация, планы коммуникаций в т.ч. стратегического назначения;
- проектная документация, полученная от заказчика;
- проектная документация, разработанная организацией;

Таким образом, в компании выявлено множество активов, связанных с информационными данными. Соответственно для них могут быть выделены следующие уязвимости:

- действия злоумышленников;
- выход из строя аппаратного обеспечения (АО);
- недостача ресурсов АО;
- конструктивные недостатки программного обеспечения (ПО);
- выход из строя ПО;

- недостача ресурсов ПО;
- похищение при передаче по линиям связи (ЛС);
- подмена при передаче по ЛС;
- отказ в облуживании ЛС;
- ошибки пользователя;
- разглашение конфиденциальной информации;
- халатное отношение к информационной безопасности;
- саботаж;
- возникновение ЧС;
- обстоятельства непреодолимой силы.

Перечень уязвимостей с указанием оценки степени вероятности возможной реализации отмеченных уязвимостей, например, «высокая», «средняя» или «низкая», приведены в приложении А, в котором отображены основные результаты оценки уязвимости активов.

Угрозы безопасности предприятия могут иметь природный или человеческий фактор, угрозы могут появиться как случайно, так и преднамеренно. Для предприятия необходимо и крайне важно не пропустить ни одной угрозы информационной безопасности, так как возможный ущерб может быть очень значителен, но и акцентировать внимание на незначительных угрозах не надо, потому как может быть задействовано крайне много средств, а ущерба предприятию может быть не нанесено.

После того как обнаружен возможный источник угрозы и сектор, подверженный угрозе (объект угрозы), надо определить возможность и размеры осуществление угрозы. Для этого необходимо учесть аналитические данные, такие как:

- частоту возникновения угрозы;
- цель угрозы, используемые ресурсы и возможности осуществления той или иной угрозы;
- насколько привлекателен ресурс, на который воздействует угроза;

- насколько возможны возникновения случайных угроз, связанных с географическим фактором, реализацией которых может являться природная или техногенная катастрофа.

Для проведения аналитики по возникшей угрозе, необходимо воспользоваться статистическими данными, если такие имеются. Статистические данные позволят определить, как часто возникает угроза и на что нацелена, какой ущерб может нанести.

По данному пункту можно сделать вывод что у данной компании есть уязвимые информационные активы, которые необходимо защищать. А для более правильного выстраивания политики информационной безопасности необходимо, определить основные проблемы и задачи защиты информации в строительной компании.

1.3 Основные проблемы и задачи защиты информации в строительной компании

В компании при работе с большим объемом конфиденциальных данных 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.

Цель защиты информации - это получение результатов от предотвращения ущерба, обусловленного утечкой или несанкционированным воздействием на информацию [23, с.46]. Эффективность защиты информации позволяет определить уровень соответствия результатов используемой системы защиты данных поставленным целям. Выделяют следующие основные виды защиты информации:

1. Защита информации от утечек – это мероприятия, направленные на сохранность и целостность конфиденциальных данных, используемых во внутреннем и внешнем документообороте предприятия.

2. 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.

3. 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 [15, с.45].

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.

Безопасность данных – это состояние защищенности данных, при котором обеспечены целостность, конфиденциальность и доступность [3, с.42]. Информационная безопасность выступает одной из главных проблем современного общества и обусловлена увеличением значимости информации в основных бизнес процессах.

Проблемы защиты информации в настоящее время связаны с дестабилизирующим воздействием внешних и внутренних угроз, возникающих в компании 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 [20, с.43]. 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.

Проблемы информационной безопасности разделяют на три основных вида [5, с.68]:

- 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.

Для того чтобы осуществить перехват конфиденциальной информации, злоумышленником используются вирусы, кейлоггеры, троянские программы, вредоносное и шпионское программное обеспечение. Проблемы защиты сети связаны с тем, что не каждая антивирусная программа может своевременно выявить возникшие угрозы в сети и это создает возможность для злоумышленника использовать сеть для достижения поставленных целей. Однако возможность перехвата информации не всегда создает возможности получения доступа к защищенным данным, с последующей модификацией. В качестве примера перехвата информации может выступать анализ сетевого трафика в сети. В данном случае злоумышленник получает информацию о сети предприятия, но возможность искажать данную информации не имеет. Проблемы безопасности данных также связаны с развитием глобальной сети Интернет, которая пользуется популярностью среди различных категорий пользователей. Усиление глобализации, а вместе с тем и информатизации

создает возможности для злоумышленника с любой точки мира создавать угрозы безопасности для компьютерной сети.

К основным задачам информационной безопасности данных относятся [28, с.45]:

- обеспечение конфиденциальности, целостности и структурированности информации;
- организация своевременного выявления и предотвращения внешних и внутренних угроз;
- внедрение организационных, инженерно-технических, аппаратно-программных методов, позволяющих усилить защиту данных;
- разработка и совершенствование политики безопасности с учетом современных тенденций развития аппаратного и программного обеспечения.

Для предприятий задачи обеспечения защиты данных являются одними из первоочередных, поскольку, выступая в качестве объекта постоянного внимания злоумышленников. Следовательно, информационная безопасность направлена на обеспечение достаточного и необходимого уровня защиты информации, что во многом определяется платежными, информационными и прочими процессами. Возникающие сбои в работе информационной структуры предприятия могут нанести значительный ущерб в области получения информации для обеспечения стабильности основных бизнес процессов. Поэтому информационная безопасность постоянно контролируется, принимаются мероприятия для управления рисками, разрабатываются документы, которые являются основной стандартизации управления защитой информации. Особое значение при обеспечении информационной безопасности уделяется формальным методам защиты информации, в основе которых находится стандартизация [8, с.27]. Главной целью стандартизации является повышение доверия, выполнение необходимых мероприятий по защите информации от возникающих угроз и внедрение методов для снижения рисков.

Для обеспечения защиты данных предприятия должны выполнять следующие задачи:

- обеспечивать высокий уровень организации и функционирования подразделений в области информационной безопасности предприятия;
- осуществлять коррекцию в области функционирования системы защиты данных;
- разрабатывать планы по управлению рисками нарушения информационной безопасности и обеспечиваться высокий уровень организации внедрения данных планов в основные бизнес процессы предприятия;
- производить коррекцию внутреннего документооборота в области защиты данных;
- принимать управленческие решения в области совершенствования системы защиты данных, а также разрабатывать и организовывать программы обучения сотрудников, мероприятия повышения осведомленности сотрудников предприятия в области защиты данных;
- осуществлять постоянный мониторинг обнаружения угроз и совершенствоваться мероприятия по их ликвидации;
- внедрять современные методы защиты данных, проводить внутренний и внешний аудит информационной безопасности;
- принимать решения в области совершенствования политики безопасности предприятия, корректироваться концепция и стратегия в области информационной безопасности.

Таким образом, были определены основные задачи, которые будут положены в основу организации системы информационной безопасности и защиты данных в рассматриваемой компании.

1.4Обоснование необходимости совершенствования обеспечения информационной безопасности и защиты информации на предприятии

При общем анализе возможных угроз предприятию можно сделать вывод о том, что текущее состояние информационной безопасности организации находится в плачевном состоянии и требует полной реорганизации. Таким

образом, в рамках разработки комплексной информационной безопасности было принято решение вести разработку в трёх направлениях.

1. Разработка административных методов обеспечения информационной безопасности.
2. Разработка программно-аппаратных методов информационной безопасности.
3. Разработки инженерно-технических методов информационной безопасности.

Первое направление подразумевает организацию трудового распорядка на предприятии; введение пропускного режима; введение регламента нахождения посторонних лиц на территории предприятия и регламента нахождения на рабочих местах сотрудников предприятия.

Разработка данного направления организации стратегии информационной безопасности согласованно с руководителем организации. Контроль над выполнением методик будет возложен на сотрудников отделов и службу охраны.

При разработке второго направления особое внимание будет уделено:

- централизованной установке антивирусного программного обеспечения;
- организацию межсетевого экрана;
- организацию средств распределения интернет - трафика;
- организацию средств централизованной авторизации пользователя;
- запрещение использования внешних накопителей;
- организацию обмена информаций между компьютерами;
- организацию распределения доступа;
- обновление программного обеспечения до актуальных стабильных версий;
- организацию резервного копирования данных.

Выполнение инструкций данного направления будет возложено на ИТ-персонал организации.

Разработка инженерно-технических средств подразумевает внедрение средств инженерно-технического характера:

- внедрение датчиков движения;
- внедрение видеокамер наблюдения;
- внедрение «тревожных кнопок».

Выполнение данных рекомендаций будет возложено на подрядные организации и организации, занимающиеся частной охранной деятельностью. Контроль над выполнением мероприятий будет проводить директор организации и завхоз офисного центра (не является сотрудником компании).

По итогу разработка всех трех направлений сводится к единым требованиям:

1. Устранить возможные угрозы информационной безопасности внутри предприятия.
2. Устранить возможные угрозы в виртуальном пространстве глобальной сети.
3. Устранить возможные угрозы свободного прохода на предприятие, и доступа к информации.

Для более тщательного изучения информации по данному вопросу необходимо рассмотреть основные положения политики информационной безопасности предприятия, опираясь на требования, которые необходимо достичь.

1.5 Основные положения политики информационной безопасности предприятия

Политика информационной безопасности предприятия представлена комплексом документов, позволяющих отразить требования к обеспечению защиты данных и основные направления предприятия по обеспечению

безопасности [10, с.65]. При создании политики безопасности можно выделить три основных уровня: верхний, средний и нижний.

Верхний уровень политики безопасности данных организации позволяет [31, с.56]:

- сформулировать и демонстрировать отношение администрации предприятия к системе защиты информации и отразить основные цели и задачи в данной области;
- разработать индивидуальные политики безопасности, инструкции и правила, с помощью которых регулируются отдельные вопросы;
- информировать сотрудников организации про основные задачи и приоритеты в области информационной безопасности.

Политика информационной безопасности среднего уровня служит для отражения отношений и требований предприятия к:

- использованию информационных систем;
- телекоммуникационных и информационных технологий, методов и подходов к обработке информации;
- участникам процессов обработки информации, от которых зависит обеспечение защиты информации на предприятии.

Нижний уровень политики безопасности служит для описания определенных процедур и документов для обеспечения информационной безопасности на предприятии.

Этапы разработки политики безопасности в организации включают:

- выполнение оценки личного отношения к угрозам безопасности со стороны собственников и сотрудников предприятия;

- проведение анализа потенциально важных информационных активов предприятия;

- выявление существующих угроз безопасности предприятия с последующей оценкой рисков.

При создании политики безопасностей всех уровней нужно придерживаться того, что разработанная политика безопасности на нижнем уровне должна соответствовать политике безопасности, приведенной на верхнем уровне. При этом в тексте политики безопасности должны быть приведены правила, не имеющие двойной смысл и он должен быть достаточно понятным для сотрудников предприятия. Важное значение для защиты информации в компании имеет политика безопасности, представленная в виде логически и семантически связанных, формируемых и анализируемых структур данных, используемых для защиты информации на всех уровнях функционирования предприятия.

Рассмотрим основные составляющие политики информационной безопасности предприятия. Под защитой в данном случае подразумевается использование приведенных в политике безопасности предприятия организационных мероприятий защиты информации. С помощью политики информационной безопасности на предприятиях выполняют внешний и внутренний аудит защиты данных, результаты которого используются для определения уровня эффективности, используемых методов и средств защиты. В свою очередь улучшение выступает в виде подстройки мероприятий политики безопасности с использованием полученных результатов проведения тестирования и мониторинга [17, с.43]. Политика безопасности в процессе функционирования предприятия должна постоянно обновляться. При этом внесенные изменения подлежат постоянному сравнению с теми методами и средствами, которые уже используются. Основные составляющие политики информационной безопасности предприятия можно представить в виде схемы, приведенной на рисунке 1.3.

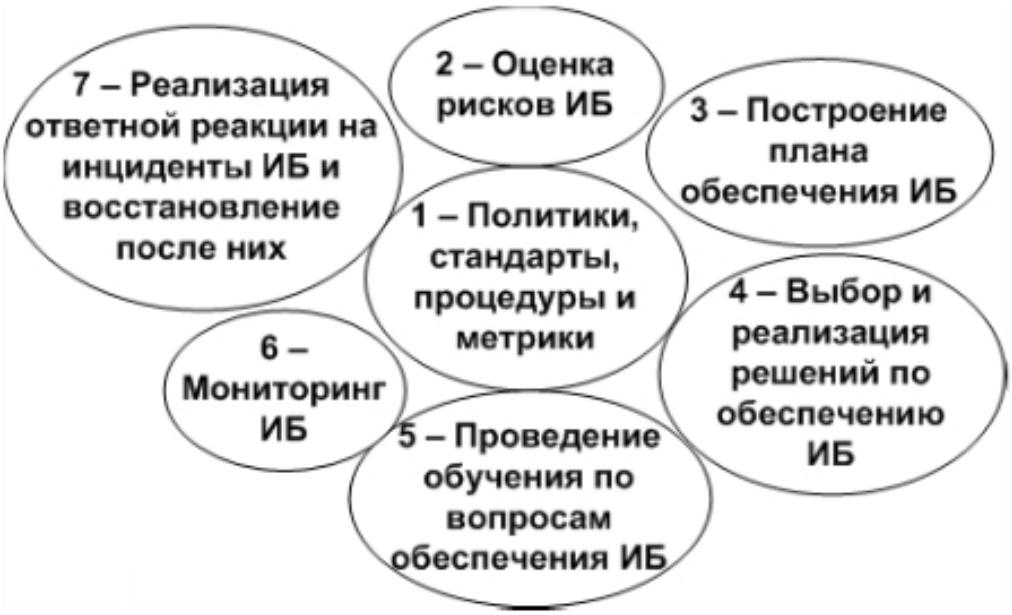


Рисунок 1.3 – Основные составляющие политики информационной безопасности предприятия

Как видно из рисунка 1.3 в политике информационной безопасности отражаются взаимосвязанные этапы организации информационной безопасности предприятия, которые представлены процедурами, позволяющими систематизировать и эффективно решать поставленные задачи для того, чтобы достичь требуемый уровень защиты данных.

На первом этапе необходимо определить границы, в рамках которых будет функционировать политика информационной безопасности предприятия, задаться критериями для оценки результатов.

На этапе анализа рисков информационной безопасности описывается состав и определяются приоритеты выбранных средств защиты с распределением их по степени важности для предприятия, идентифицируются уязвимости активов предприятия и определяться ущерб. Результаты анализа рисков информационной безопасности предприятия будут применяться в виде основы для планирования работы системы информационной безопасности, выбора наиболее эффективной стратегии и тактики. Для повышения эффективности политики безопасности применяются такие приемы как

групповое определение объектов безопасности, косвенное определение с использованием верительных атрибутов и мандатное управление доступом.

Многие предприятия используют глобальную и локальную политики безопасности, основанные на принципах управления безопасностью информации. Глобальная политика информационной безопасности направлена на обеспечение защиты информации на уровне бизнес-процессов компании, а локальная политика формируется на уровне защиты данных предприятия.

В глобальной политике предприятия представлены правила безопасности, описывающие возможное взаимодействие между объектами, для которых необходимо обеспечение защиты информации. В общем виде глобальную политику безопасности можно представить в виде структуры приведенной на рисунке 1.4.

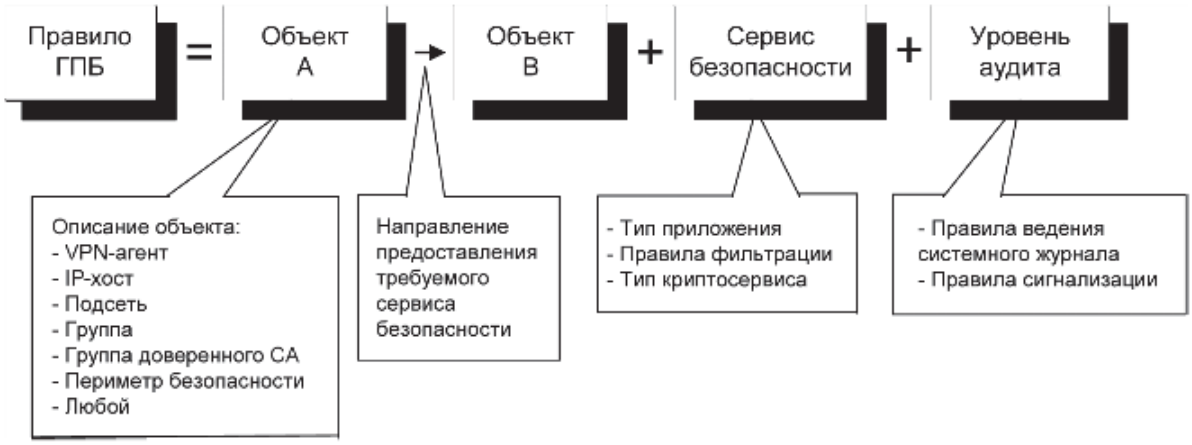


Рисунок 1.4 – Общая структура глобальной политики безопасности предприятия

За счет использования приведенной на рисунке 1.4 глобальной политики для обеспечения защиты информации выполняют правила аутентификации объектов, обмен ключами, ведут запись результатов событий безопасности в специальный журнал и учет рисков безопасности данных. В качестве объектов для глобальной политики безопасности выступают отдельные рабочие станции и подсети, включающие в свой состав структурные подразделения предприятия.

В глобальной политике безопасности компании правила функционально разбиваются на следующие группы:

- правила VPN, которые реализованы с использованием протоколов IPSec. В качестве агента исполнения данных правил выступает драйвер VPN, установленный в стеках клиентских устройств или шлюзах безопасности;

- правила пакетной фильтрации, позволяющие обеспечить фильтрацию пакетов типов stateless и stateful;

- прокси - правила, с включением антивирусной защиты, которые отвечают за фильтрацию трафика, который передается через прикладные протоколы. В данном случае в качестве исполнительного агента выступает прокси-агент;

- правила авторизованного доступа, с применением правил однократного входа, позволяющие обеспечить работу пользователей по паролям. Данные правила выполняются агентами различных уровней от VPN-драйвера до прокси-агентов. В качестве агентов выполнения таких правил защиты информации выступают системы авторизации;

- правила, которые отвечают за протоколирование событий, уязвимостей в системе защиты информации. В компании политика ведения журналов событий выполняется агентом протоколирования, а в качестве исполнителей выступает полностью вся информационная система.

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.

1.6 Оценка существующих и планируемых средств защиты

До текущего момента на объекте не производилась целенаправленная разработка и внедрение политики информационной безопасности.

Использование методов защиты информации было эпизодическим и сводилось к установке бесплатных антивирусных программы и физической защите (запирание помещений на ночь). Данная халатность со стороны информационно-технического персонала привела не нескольким инцидентам, приставлявшим угрозу для деятельности организации. Поэтому было принято решение о необходимости разработки комплексной политики информационной безопасности.

Ниже будет рассмотрена существовавшая защита информационной безопасности с точки зрения:

- программного обеспечения;
- технического обеспечения.

Результаты обследования объекта на предмет наличия информационной безопасности внесены в таблицу 1.2.

Таблица 1.2 - Анализ выполнения основных задач по обеспечению информационной безопасности

Основные задачи по обеспечению информационной безопасности	**Степеньвыполнения**
обеспечение безопасности деятельности, защита информации и сведений, являющихся коммерческой тайной;	Низкая
организация работы по правовой, организационной и инженерно-технической (физической, аппаратной, программной и математической) защите коммерческой тайны;	Отсутствует
организация специального делопроизводства, исключающего несанкционированное получение сведений, являющихся коммерческой тайной;	Отсутствует
предотвращение необоснованного допуска и открытого доступа к сведениям и работам, составляющим коммерческую тайну;	Отсутствует
выявление и локализация возможных каналов утечки конфиденциальной информации в процессе повседневной производственной деятельности и в экстремальных (авария, пожар и др.) ситуациях;	Не проводится

Продолжение таблицы 1.2

обеспечение режима безопасности при осуществлении таких видов деятельности, как различные встречи, переговоры, совещания, заседания и другие мероприятия, связанные с деловым сотрудничеством на национальном и международном уровне;	Не обеспечивается
обеспечение охраны территории, зданий помещений, с защищаемой информацией.	Вахтёр без спецоборудования и лицензии на охранную деятельность.

Из таблицы 1.2 видно, что положение компании по отношению к стандартам защиты информации весьма низкое, т.е. в случае хищения данных компания может понести колоссальные потери. Данные, указанные в таблице, показывают, что выбранное направление разработки информационной безопасности является актуальным и крайне необходимым.

Таким образом, можно сделать вывод, что компания нуждается в разработке новой политики информационной безопасности, и выбранные решения являются актуальными на данном предприятии.

В первой главе ВКР даны определения основным терминам и понятиям, связанным с политикой защиты информации, дано описание предприятия, проведен сравнительный анализ системы безопасности, получены следующие авторские выводы:

- 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;
- главной целью стандартизации является повышение доверия, уровня стабильности работы сети, выполнение необходимых мероприятий по

защите информации от возникающих угроз и внедрение методов для снижения рисков;

- также необходимо разработать документы, которые составят основу политики информационной безопасности.

Полученные результаты и сформулированные выводы позволяют перейти к рассмотрению материала второй главы, посвященной описанию и определению классификации основных угроз информационной безопасности.

Глава 2 РАЗРАБОТКА ПОЛИТИКИ ИНФОРМАЦИОННОЙ БЕЗОПАСНОСТИ СТРОИТЕЛЬНОЙ КОМПАНИИ

2.1 Политика информационной безопасности в строительной компании

Политика информационной безопасности определяет систему взглядов на проблему обеспечения безопасности информации и представляет собой систематизированное изложение целей и задач защиты, правил, процедур, практических приемов и руководящих принципов в области информационной безопасности, принципов построения, организационных, технологических и процедурных аспектов обеспечения безопасности информации в компании [32].

Основными объектами системы информационной безопасности в компании являются:

- информационные ресурсы, необходимые для работы. Информация предприятия как ресурс имеет очень большое значение для стабильного развития компании. А стабильное развитие компании – это благополучие ее сотрудников, поэтому информацию необходимо подвергать тщательной защите. И данную защиту возможно осуществить согласно политике информационной безопасности;
- информационные технологии, регламенты и процедуры сбора, обработки, хранения и передачи информации, персонал разработчиков и пользователей системы и ее обслуживающий персонал;
- информационная инфраструктура, включающая системы обработки и анализа информации, технические и программные средства ее обработки, передачи и отображения, в том числе каналы информационного обмена и телекоммуникации, системы и средства защиты информации, объекты и помещения.

Основной целью политики информационной безопасности является защита субъектов информационных отношений от возможного нанесения им материального, физического, морального или иного ущерба, посредством случайного или преднамеренного воздействия на информацию, ее носители,

процессы обработки и передачи, а также минимизация уровня операционного и других рисков [32].

Кроме того, целями информационной безопасности компании являются:

- защита экономических данных компании;
- защита данных о разработках проектов;
- защита конфиденциальности информации клиентов и сотрудников;
- соответствие веб - сервисов, автоматизированных систем и внутренних сетей стандартам защиты информации;
- защита имущества предприятия.

Для достижения основной цели обеспечения информационной безопасности необходимо решить следующие задачи [32]:

- своевременное выявление, оценка и прогнозирование источников угроз информационной безопасности, причин и условий, способствующих нанесению ущерба заинтересованным субъектам информационных отношений;
- создание механизма оперативного реагирования на угрозы безопасности информации и негативные тенденции;
- создание условий для минимизации и локализации наносимого ущерба неправомерными действиями физических и юридических лиц, ослабление негативного влияния и ликвидация последствий нарушения безопасности информации;
- защиту от вмешательства в процесс функционирования информационной системы посторонних лиц (доступ к информационным ресурсам должны иметь только зарегистрированные в установленном порядке пользователи);
- разграничение доступа пользователей к информационным, аппаратным, программным и иным ресурсам, то есть защиту от несанкционированного доступа;
- обеспечение аутентификации пользователей, участвующих в информационном обмене (подтверждение подлинности отправителя и получателя информации);

- защиту от несанкционированной модификации используемых программных средств, а также защиту системы от внедрения несанкционированных программ, включая компьютерные вирусы;
- защиту информации ограниченного пользования от утечки по техническим каналам при ее обработке, хранении и передаче по каналам связи;
- обеспечение криптографических средств защиты информации.

Решение обозначенных задач может быть достигнуто:

- строгим учетом всех подлежащих защите ресурсов (информации о клиентах, автоматизированных рабочих мест сотрудников);
- учет всех действий сотрудников, осуществляющих обслуживание и модификацию программных и технических средств корпоративной информационной системы;
- разграничением прав доступа к ресурсам в зависимости от решаемых задач сотрудниками;
- четким знанием и строгим соблюдением всеми сотрудниками требований организационно-распорядительных документов по вопросам обеспечения безопасности информации;
- персональной ответственностью за свои действия каждого сотрудника, в рамках своих функциональных обязанностей;
- применением физических и технических (программно-аппаратных) средств защиты ресурсов системы и непрерывной административной поддержкой их использования.

Данная политика распространяется на всех сотрудников предприятия и требует полного исполнения. Данная политика укрепляет общую политику безопасности компании. Весь персонал должен быть ознакомлен и подотчетен за информационную безопасность в отношении своих должностных полномочий.

Генеральный директор отвечает за обеспечение соответствующей проработки информации во всей организации. Каждый начальник отдела отвечает за то, чтобы сотрудники, работающие под его руководством,

осуществляли защиту информации в соответствии со стандартами организации. Начальник отела безопасности информирует группу руководителей высшего звена, оказывает консультативную помощь сотрудникам организации и обеспечивает доступность отчетов о состоянии информационной безопасности. Каждый сотрудник организации отвечает за информационную безопасность как часть выполнения своих должностных обязанностей.

Таким образом, определены основные задачи по организации политики информационной безопасности в строительной компании и пути их решения.

2.2 Организационные меры обеспечения политики информационной безопасности предприятия

При построении информационной безопасности предприятия используются международные стандарты информационной безопасности ISO 17799 ("Нормы и правила при обеспечении безопасности информации"). Данные стандарты описывают рекомендации общего характера по обеспечению информационной безопасности, обеспечивающие основной уровень информационной безопасности систем. В стандарте ISO 17799 описаны нормы, которые необходимо изучить и учесть при создании политики информационной безопасности и проектировании конкретных мер обеспечения защиты данных.

Стандарт ISO 17799 состоит из разделов, регламентирующих многие направления обеспечения безопасности информационных систем:

- политика информационной безопасности регламентирует важность поддержки руководством компании утвержденной системы организации информационной безопасности;
- рекомендации по политике информационной безопасности предприятия описываются в разделе организационные вопросы;
- меры обеспечения информационной безопасности описаны в разделе классификация информационных ресурсов;
- воздействие человеческого фактора и нормы, разработанные для уменьшения риска безопасности, описаны в разделе управление персоналом;

- реализация физической безопасности регламентирует действия по обеспечению безопасности компонентов информационной системы;
- действия при работе с серверами, рабочими станциями и т.д. описаны в разделе администрировании информационных систем;
- необходимость разграничения прав при работе с информацией регламентирует управление доступом;
- основные рычаги информационной безопасности систем описывает раздел разработки и сопровождения информационных систем;
- постоянная работа предприятия без перерывов описывает термин обеспечения непрерывности бизнеса;
- общие требования к политике информационной безопасности описывает термин обеспечения соответствия предъявляемым требованиям.

Политика информационной безопасности должна быть доведена до сведения всех пользователей организации в форме, являющейся актуальной, доступной и понятной для читателей, которым она предназначена [32].

Политика информационной безопасности должна быть частью более общей документированной политики. Если политика информационной безопасности распространяется за границы организации, должны быть приняты меры для предотвращения раскрытия конфиденциальной информации.

Степень информационной безопасности предприятия определяется правилами соблюдение политики информационной безопасности. Для компании политика информационной безопасности представлена следующими нормативными документами:

1. Приказ №214-BS «Об административной защите предприятия». Данный приказ регламентирует применение административных мер в целях предотвращения утечек информации.

2. Приказ №332-AD «О создании службы информационной безопасности».

3. Приказ №322-AG «О соблюдении информационной безопасности в офисах и на объектах проведения работ».

4. «Рекомендации по повышению качества информационной безопасности».

Данные нормативные документы полностью регламентируют правила использования компьютерной техники и информационных ресурсов с точки зрения политики информационной безопасности предприятия.

2.3Аппаратные и программные средства обеспечения информационной безопасности в строительной компании

Электронные и электронно-механические устройства, входящие в состав технических средств охраны, являются аппаратными средствами обеспечения информационной безопасности. Аппаратные средства, работающие вместе с программными средствами или самостоятельно, выполняют задачи необходимые для построения информационной безопасности. Электронные и электронно-механические устройства являются аппаратными средствами обеспечения информационной безопасности. а не инженерно-техническими средствами, если они в обязательном порядке входят в состав технических средств политики информационной безопасности.

Аппаратными средствами политики информационной безопасности являются:

- устройства ввода биометрических данных распознавания;
- устройства идентификации сотрудника;
- устройства кодирования информации;
- электронные замки и блокираторы, не дающие бесконтрольно включать рабочие станции.

К вспомогательным средствам защиты информации относятся:

- средства уничтожения магнитных носителей и информации на них;

- средства сигнализации, предупреждающие о несанкционированных действиях пользователей.

К программным средствам защиты информации относятся программы, входящие в состав программного обеспечения, необходимого для защиты данных. К данным средствам защиты информации возможно отнести:

- программы распознавания пользователей;
- программы определения зоны доступа к ресурсу;
- программы криптографической защиты информации;
- программное обеспечение: баз данных, компьютерных средств;
- программы, защищающие информацию от незаконного доступа и копирования.

Идентификация пользователей в политике информационной безопасности понимается как 100% определение индивидуального и уникального имени пользователя, а аутентификация служит для того, чтобы определить 100% принадлежность пользователю представленного имени.

Как пример программ, помогающих в защите информации, могут выступать:

- программы удаления оставшейся информации (во временных файлах, оперативной памяти и т.д.);
- аудиторские программы событий, которые описывают произошедшие угрозы, журналы регистрации событий, которые могут представляться как доказательство произошедших угроз;
- программы, создающие возможные события, при которых осуществляется имитация работы с нарушителем;
- программы тестирования защищенности.

Для защиты локальной вычислительной сети необходимо пользователей разделить на группы с соответствующими правами:

1. Administrator – администраторы сети (создание и управление политиками информационной безопасности, глобальные настройки сети и т.д.).

2. Manager – учётные запись для повседневного обслуживания информационно-вычислительной техники.

3. User – учётная запись стандартного пользователя (сотрудника компании) с ограниченными правами.

4. Security – ограниченная учёная запись (в случае необходимости доступа не сотрудников организации).

Для идентификации пользователя требуется ActiveDirectory на базе сетевой операционной системы, где для каждого пользователя должна быть создана уникальная запись, и каждая запись была включена в соответствующую группу. Тем самым осуществляется разграничение доступа (табл. 2.1)

Таблица 2.1 – Группы пользователей и их права

Действия	**Security**	**User**	**Manager**	**Administrator**
Создание и изменения групп пользователей	Нет	Нет	Нет	Да
Изменение настроек сети	Нет	Нет	Нет	Да
Подключение к сети новых рабочих станций	Нет	Нет	Нет	Да
Изменение настроек серверов	Нет	Нет	Нет	Да
Изменение прав доступа к каталогам и резервным копиям	Нет	Нет	Нет	Да
Установка приложений	Нет	Нет	Да	Да
Доступ в Интернет	Нет		Да	Да
Количество трафика (в месяц)	0	100	1000	1000
Возможность скачивать файлы	Нет	Нет	Да	Да
Запись	Только в «Мои документы»	«Мои документы», «Рабочий стол», «Для всех», «Сетевая»	Любая папка на локальном компьютере	Любая папка на любом компьютере в сети.

Продолжение таблицы 2.1

Подключение внешних флеш-дисков, Внешних дисков.	Нет	Нет	Да	Да
Подключение CD/DVD-ROM, Флоппи-диска	Нет	Нет	Да	Да
Использование ICQ	Нет	Да	Да	Да
Доступ к FTP	Нет	Нет	Нет	Да
Доступ к POP3	Нет	Да	Да	Да
Доступ к SMTP	Нет	Да	Да	Да
Доступ к SSL	Нет	Да	Да	Да
Доступ к SOCKS	Нет	Нет	Нет	Да

Для снижения уязвимости программных средств было решено оценить степень подготовки операционных систем. Для этого были приняты следующие меры:

1. Произведена замена устаревших операционных систем на новые операционные системы;

2. Там, где замена операционных систем нецелесообразна, произведено обновление существующих операционных систем путём установки сервис - паков последних версий.

Для повышения качества антивирусной защиты было принято решение внедрить более совершенный антивирус. Контроль интернет - трафика будет осуществляться при помощи прокси-сервера, который одновременно будет служить и фаерволом.

Можно сделать вывод, что по отдельности программный комплекс и аппаратный комплекс мало эффективны, поэтому необходимо два этих рычага защиты информации использовать вместе, тем самым получив программно-аппаратный комплекс. Поэтому считаю необходимым рассмотреть структуру программно-аппаратного комплекса, используемого для обеспечения информационной безопасности данных в организации.

2.4 Комплекс программно-аппаратных средств обеспечения информационной безопасности в строительной компании

Программно-аппаратный комплекс – это набор технических и программных средств, работающих совместно для выполнения одной или нескольких сходных задач [31].

Программный комплекс на данном предприятии включает следующие компоненты: операционная система Windows XP, антивирус Dr. Web Enternet Security. В программном комплексе парольная защита организована стандартным разграничением доступа пользователей Windows, передача данных осуществляется в интернет без использования защищенного соединения по технологии VPN. Для более расширенного функционирования комплекса на сервере необходимо произвести: настройку межсетевого экрана, установку прокси сервера, установку почтового сервера.

Аппаратный комплекс на предприятии представлен:

- персональные электронные вычислительные машины Office Cor 2 duo E7500, а также Celeron 430;
- Hub Dlink DES - 1005D/E;
- принтеры HP DeskJet 2050;
- сканеры Genius G Pen.

Программный и аппаратный комплекс являются одним рабочим комплексом, именуемый в дальнейшем программно-аппаратный комплекс. Для понимания сущности программно-аппаратного комплекса, предлагаемого для строительной организации, рассмотрим его структуру, представленную на рисунке 2.1.

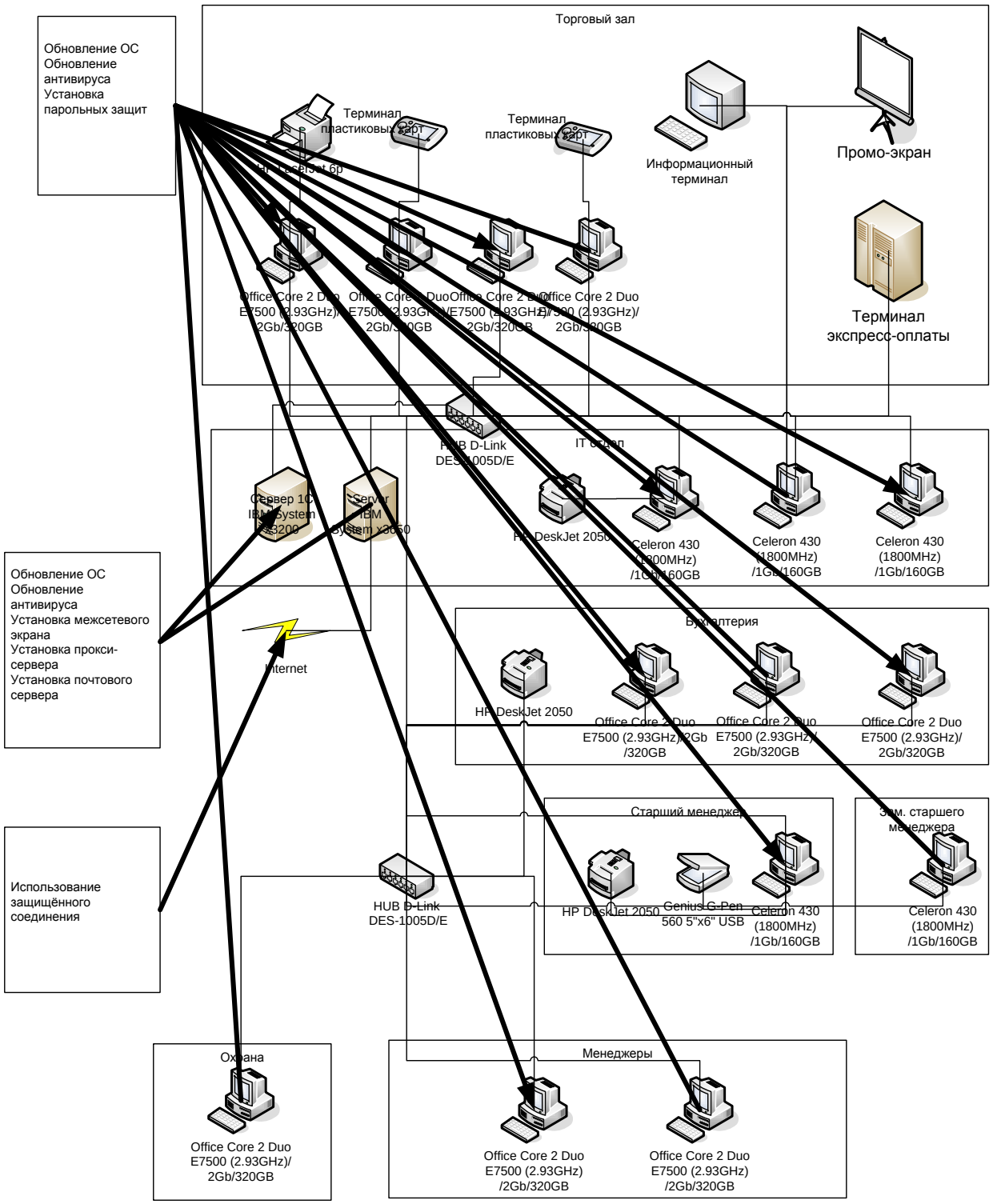


Рисунок 2.1 - Структура программно-аппаратного комплекса

Из представленной схемы видно, что в целях повешении информационной безопасности были проведены мероприятии по усилению безопасности сети предприятия, представленные в таблице 2.2.

Таблица 2.2 – Проведенные мероприятия по усилению безопасности сети предприятия

Объект	**Мероприятия**
Сервер	Обновление ОС Обновление антивируса Установка межсетевого экрана Установка прокси-сервера Установка почтового сервера
Рабочие станции	Обновление ОС Обновление антивируса Установка парольных защит
Соединения	Использование защищённого Интернет-соединения

Комплексная политика защиты информации включает в себя инженерно-техническое обеспечение компьютерной безопасности, которая рассматривается как элемент предотвращения компьютерных преступлений. Инженерно-техническая защита рассматривается как комплекс мер, рычагов, технических средств и мероприятий по обеспечению информационной безопасности.

Для противостояния техническим средствам разведки на предприятиях используют: криптографические, аппаратные, аппаратно-программные, физические и программные средства защиты информации.

Под физическими методами защиты информации подразумевается охрана помещений и здания компании, помещения с рабочими станциями, а также средства компьютерной техники и носителей информации.

Под аппаратными методами защиты информации подразумевается оборудование в виде отдельных технических средств, компьютерной техники, которые используются для защиты этих систем.

Таким образом, изменяется структура инженерно-технического комплекса информационной безопасности и защиты информации предприятия, изображенная на рисунке 2.2.

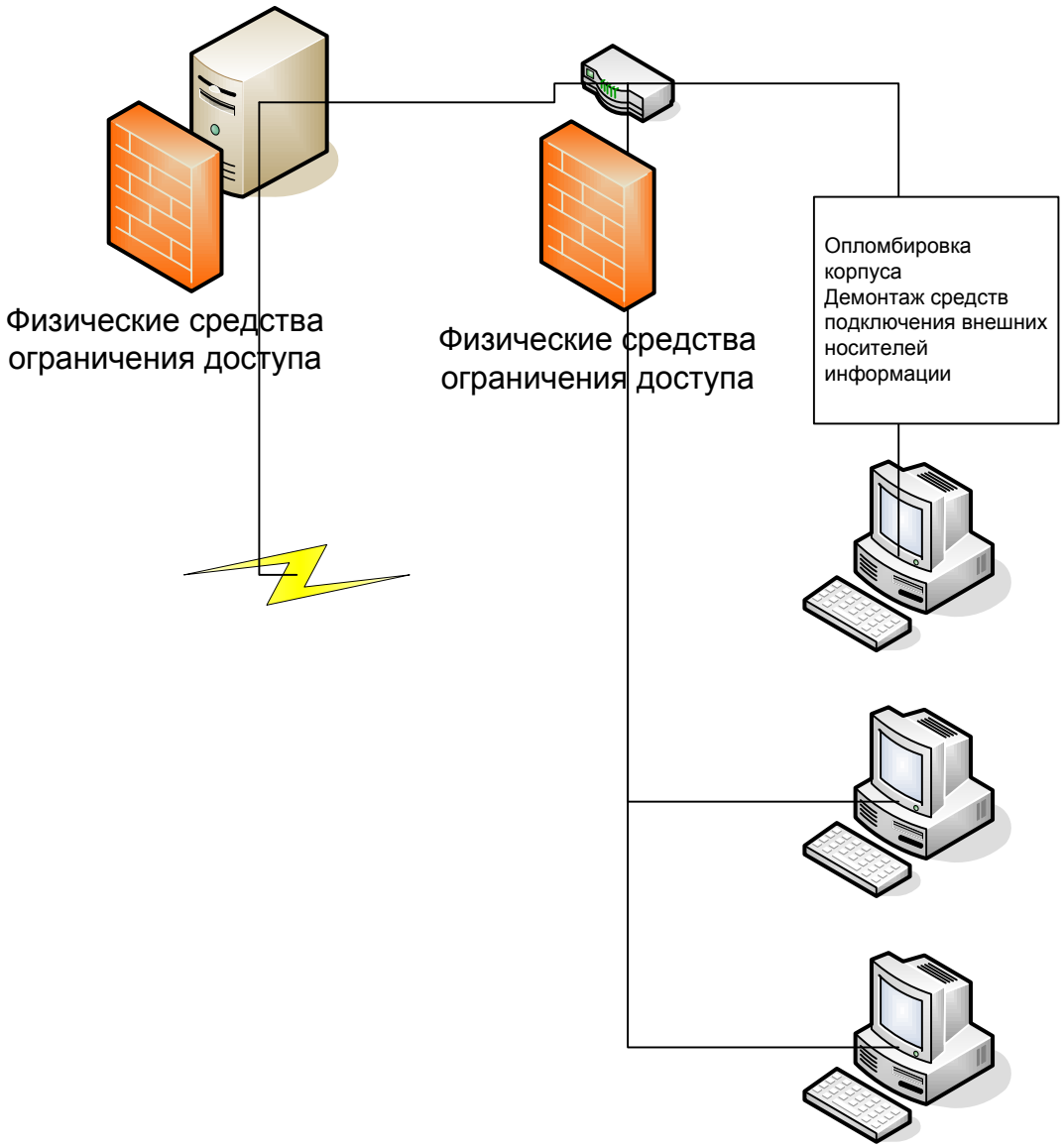


Рисунок 2.2 - Структура инженерно-технического комплекса

С помощью инженерно-технического комплекса на предприятии мы ограничиваем доступ в сеть и производим разграничение доступа к базе данных. Чтобы исключить копирование данных на внешние носители на всех персональных рабочих станциях необходимо произвести опломбирование корпуса и демонтаж средств подключения внешних носителей. Для этого, в целях обеспечения информационной безопасности компьютерной сети были проведены следующие мероприятия (см. табл. 2.3).

Таблица 2.3 – Произведенные мероприятия обеспечения информационной безопасности

Объект	**Мероприятия**
Сервер	Физические средства ограничения доступа
Узлы сети	Физические средства ограничения доступа
Рабочие станции	Опломбировка корпуса с применением специальных запорных устройств Демонтаж средств подключения внешних носителей информации

Обязательными при представлении комплекса инженерно-технических средств являются следующие задачи [35]:

- предотвращение проникновения злоумышленника к источникам информации с целью её уничтожения, хищения или изменения;
- защита носителей информации от уничтожения в результате воздействия стихийных сил и прежде всего, пожара и воды (пены) при его тушении;
- предотвращение утечки информации по различным техническим каналам.

Для обеспечения эффективной инженерно-технической защиты информации необходимо определить:

- что защищать техническими средствами в данной организации, здании, помещении;
- каким угрозам подвергается защищаемая информация со стороны злоумышленников и их технических средств;
- какие способы и средства целесообразно применять для обеспечения информационной безопасности с учётом как величины угрозы, так и затрат на её предотвращение;
- как организовать и реализовать техническую защиту информации в организации [35].

Для организации были выделены следующие объекты инженерно-технической защиты, которые были разделены по классам защиты:

1. Объекты первого (наивысшего класса) защиты. К данным объектам защиты были отнесены все носители информации, уничтожение или хищение которых приведёт к остановке деятельности фирмы, несению крупных финансовых потерь, возникновению конфликтов с законом и т.д.

2. Объекты второго класса защиты. К данным объектам были отнесены объекты, уничтожение или хищение которых повлечёт осложнения в работе компании, вызвать временные простои.

3. Объекты третьего класса защиты, к данным объектам были отнесены объекты, уничтожение или хищение которых незначительно скажется или никак не отразиться на деятельности фирмы.

Данные по важности защищаемых объектов сведены в таблицу 2.4

Таблица 2.4 Распределение по важности защищаемых объектов

№ п/п	**Класс**	**Наименованиеобъекта**
1	1	Компьютерруководителя
2	1	Компьютерсекретаря
3	1	Компьютергл. бухгалтера
4	1	Документы руководителя
5	1	Документы секретаря
6	1	Документы гл. бухгалтера
8	1	Серверы
10	2	Документы бухгалтерии
11	2	Документы производственногоотдела
12	2	Прочиедокументы
13	3	Компьютеры программиста, системного администратора
14	3	Компьютеры бухгалтерии
15	3	Компьютеры производственного отдела
16	3	Компьютеры отдела кадров
17	3	Прочие носители информации

Для охраны решено было задействовать следующие инженерно-технические методы для обеспечения информационной безопасности:

1) установка камер видеонаблюдения;

2) установка детекторов движения;

3) установка систем оповещения о пожаре;

4) установка систем автоматического пожаротушения;

5) установка средств пассивной защиты от огня.

Данные средства позволяют сократить риск потери, как информации, так и ценного имущества, в результате попытки умышленного похищения информационных носителей или материальных ценностей либо при возникновении возгорания. От использования средств защиты от прослушивания и прочих средств шпионажа, решено было отказаться, поскольку их приобретение, установка и обслуживание дорого обойдутся предприятию.

Для обеспечения информационной безопасности было определено три класса объектов, требуемых защитой, как необходимый список мер и перечень действий для устранения проблем безопасности в системе предприятия. Но было принято решение отказаться от средств зашиты от прослушки и прочих средств зашиты от шпионажа.

Реализация разработанных мер информационной безопасности с применением конкретных средств описана в таблице 2.5.

Таблица 2.5-Реализация разработанных мер информационной безопасности

Объект	Мероприятие	Суть проведения
Сервер	Обновление ОС	Установка последних обновлений серверных операционных систем для устранения уязвимостей защиты, настройка автоматических обновлений.
Сервер	Обновление антивируса	Установка современной лицензионной антивирусной NOD 32, с настрой кой постоянных обновлений антивирусных баз.
Сервер	Установка межсетевого экрана	Установка межсетевого экрана Microsoft ISA Server
Сервер	Установка прокси-сервера	Установка прокси-сервера Microsoft ISA Server

Продолжение таблицы 2.5

Сервер	Установка почтового сервера	Установка почтового сервера Microsoft Exchange
Рабочая станция	Обновление ОС	Для машин с Windows XP и Windows 2000 смена ОС на Windows8, настройка автоматических обновлений.
Рабочая станция	Обновление антивируса	Установка современной лицензионной антивирусной NOD 32, с настрой кой постоянных обновлений антивирусных баз.
Рабочая станция	Использование парольных защит	Заведение групп пользователей в Microsoft Active Directory с последующей генерацией индивидуальных паролей и настройкой групповых политик.
Соединение	Использование защищённого Интернет-соединения для обмена информацией с главным офисом	Для безопасного обмена данными с главным офисом было использовано защищенное VPN соединение с локальной сетью основного офиса защищённое 128 битным шифрованием трафика

Таким образом, использование разработанных мер безопасности позволит организовать политику информационной безопасности, а также скорректировать структуру реализуемого аппаратно-программного комплекса.

Структура программного состава комплекса приведена на рисунке 2.3.

В структуру обновленного программного комплекса включено:

1) сервер 1С: работает на операционной системе Windows Server 2008, на нем располагается база программы 1С Предприятие 8.1; антивирус, установленный на данном сервере NOD 32. Через службу каталогов Active Directory осуществляется распределение доступа;

2) сервер IBM - работает на операционной системе Windows Server 2008, на нем располагается файл-сервер, а также Firewall. Доступ в интернет осуществляется через Firewall, на файл-сервер стекается информация от прикладных программ с рабочих станций;

3) рабочие станции 1-ого типа работают на операционной системе Windows 7, на них установлена: программа 1С предприятие (клиент), Microsoft Office 2013, а также браузер Internet Explorer 11, антивирус NOD 32;

4) рабочие станции 2-ого типа работают на операционной системе Windows 8, на них установлена: программа 1С предприятие (клиент), Microsoft Office 2013, а также браузер Internet Explorer 11, антивирус NOD 32.

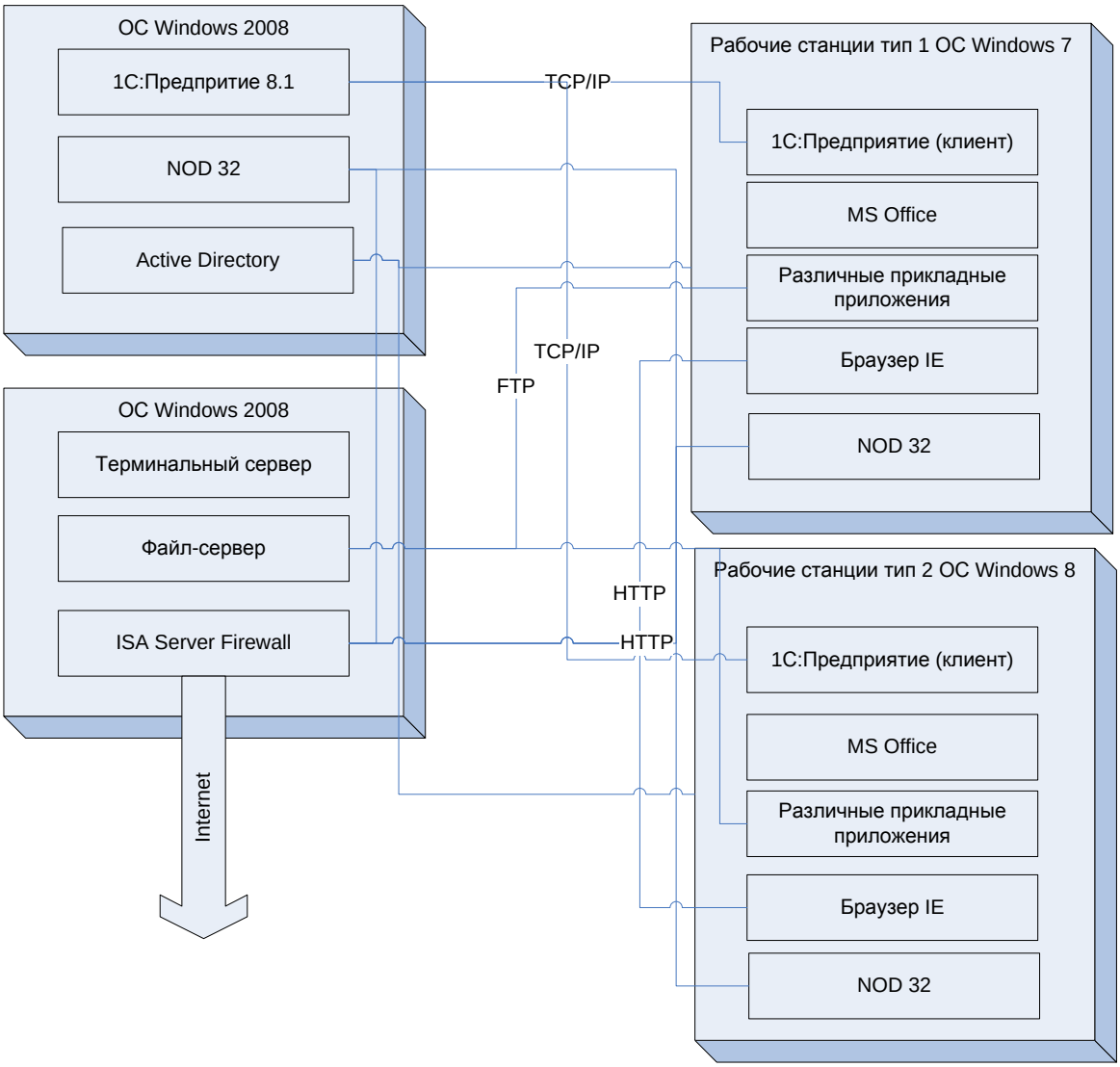


Рисунок 2.3 - Структура обновленного программного комплекса

Для реализации разработанных мер и создания защищенного интернета, а также для ограничения доступа к серверу узлам сети и рабочим станциям необходимо произвести мероприятия по реализации разработанных мер

ограничения доступа. Реализация разработанных мер по ограничению доступа и средства контроля доступа к ресурсу описана в таблице 2.6.

Таблица 2.6 Реализация разработанных мер по ограничению доступа

Объект	**Мероприятие**	**Суть проведения**
Сервер	Ограничение физического доступа	Оборудование помещения для расположения серверов. Оборудование данного помещения запирающимися дверями и системами сигнализации.
Узлы сети	Ограничение физического доступа	Расположение сетевых кабелей в специальных каналах для исключения возможности свободного доступа. Расположение важного сетевого оборудования на территории серверной либо в специальных запирающихся коробах.
Рабочие станции	Опломбировка корпусов и использованием специальных запирающих устройств	Опломбировка корпусов всей компьютерной техники с целью своевременного обнаружения попыток несанкционированного внедрения либо извлечения устройств. Применение запирающих устройств на корпусах, где такое предусмотрено конструкцией корпуса.

Реализация инженерно-технической защиты информации представлена следующими задачами:

- установка камер видеонаблюдения;
- установка детекторов движения;
- установка систем оповещения о пожаре;
- установка систем автоматического пожаротушения;
- установка средств пассивной защиты от огня.

Установка камер видеонаблюдения в офисе продемонстрированная следующим планом (см. рис. 2.4).

В данном случае в офисе компании были установлены 4 видеокамеры Vision Hi-Tech VB32BS-HVF49, в местах потенциального входа посетителей:

- камера № 1 установлена на противоположной стене коридора и в поле её обзора попадают все люди, входящие или выходящие из лифта;

- камера №2 установлена так, что в её обзор попадают люди, попадающие в помещение офиса по лестнице;
- камера №3 установлена так, что в поле её обзора попадают все люди, входящие приёмную и кабинет директора;
- камера №4 фиксирует всех людей, пытающихся попасть в помещение через балкон.

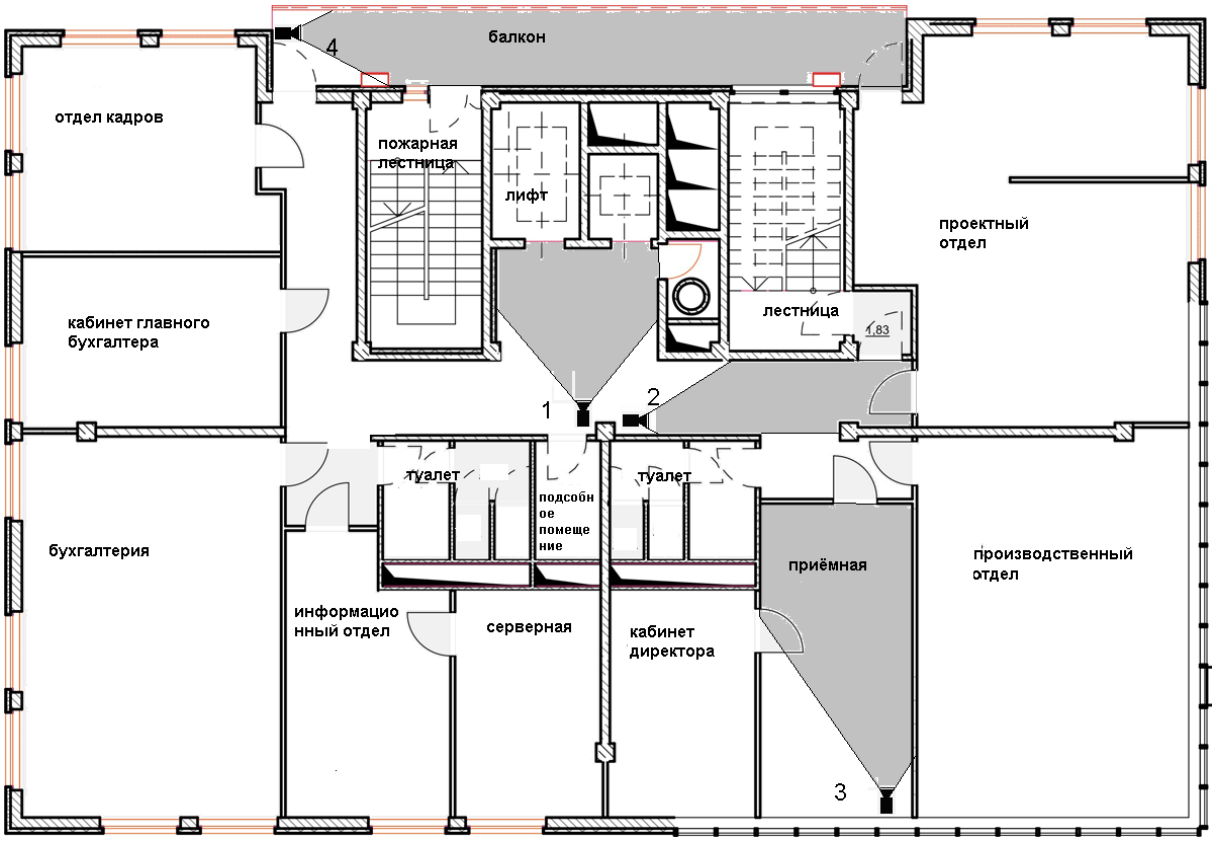


Рисунок2.4 - План установки видеокамер

Таким образом, камеры фиксируют лицо каждого человека, который входит в офис. Видеоданные с камер выводятся на монитор охраны и записываются на специальный носитель информации с периодичностью перезаписи 14 дней.

Для защиты офиса в ночное время от проникновения злоумышленников через двери и окна в офисе были установлены 11 детекторов движения в следующих местах:

- отдел кадров;
- кабинет главного бухгалтера; бухгалтерия;
- информационный отдел;

- серверная;
- кабинет директора; приёмная;
- производственный отдел;
- проектный отдел;
- коридор.

Были выбраны детекторы IS215T (Ademco) (см. рис. 2.5) со следующими техническими характеристиками:

- зона обнаружения 12 х.12 м с контролем «под собой»;
- диаграмма направленности типа «широкий угол»;
- два уровня чувствительности;
- высокая устойчивость к воздействию белого света свыше 6000 лк;
- диапазон рабочих температур -10°С– +55°С;
- размеры 87 х 62 х 40 мм.

Схема расположения детекторов указана на плане (см. рис. 2.5), где цветом показаны зоны покрытия.

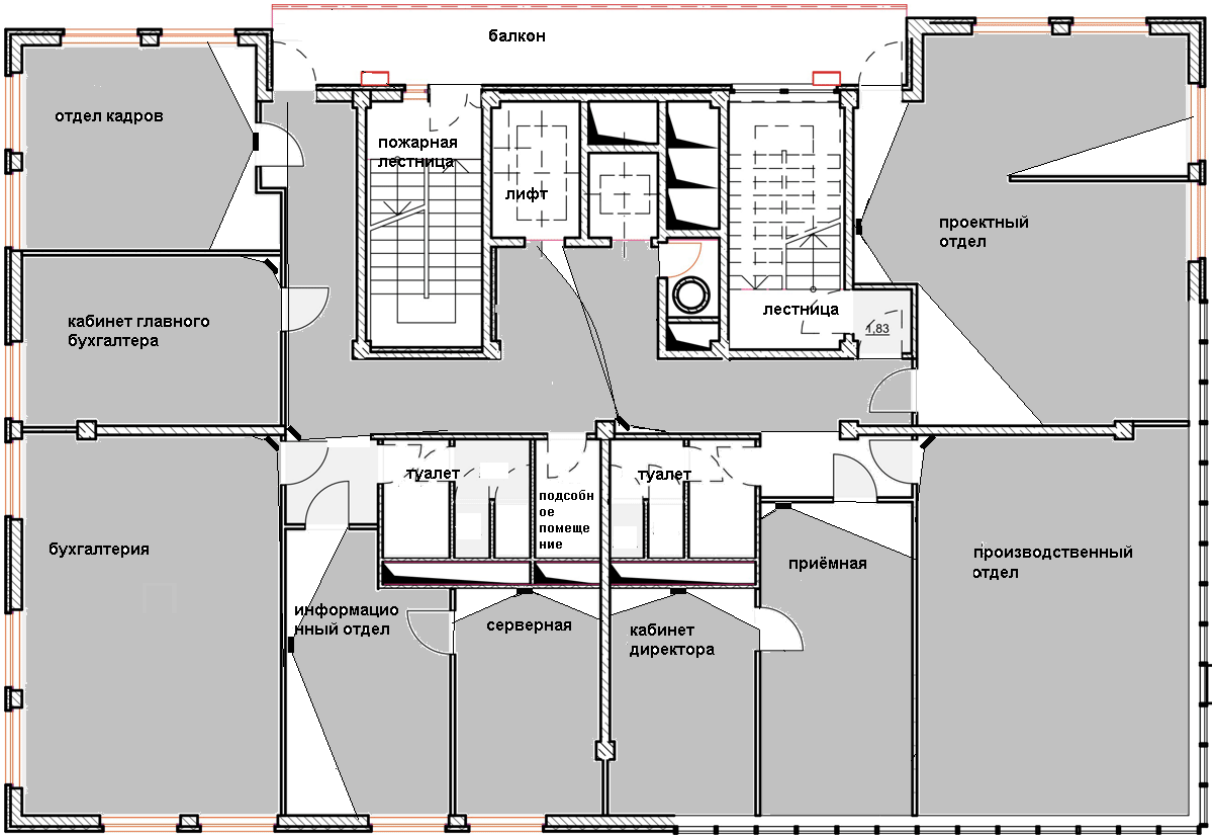


Рисунок2.5 - Схема расположения детекторов

Как видно из плана, практически весь офис при таком расположении является охраняемой зоной.

Все предложенные средства защиты информации являются актуальными и необходимыми для предприятия.

2.4 Криптографические методы и средства защиты данных

Криптография представляет собой научное направление, позволяющее исследовать методы обеспечения конфиденциальности, целостности информации, аутентификации, а также невозможность отказа от авторства.

Криптография подразделяется на два направления:

- шифрование информации, связанное с обратимым преобразованием данных для того чтобы своевременно установить неавторизованных пользователей и соблюдать конфиденциальность передаваемых данных;
- создание алгоритмов электронной цифровой подписи.

Применение электронной цифровой подписи в предприятиях предусматривает выполнение трех основных правил [7, с.63]:

- подписание документа с помощью электронной подписи может выполнять наделенный соответствующими полномочиями сотрудник;
- в случае возникновения внештатной ситуации должна быть предусмотрена возможность установления подлинности электронной подписи;
- электронная подпись в сети обязательно должна быть закреплена штампом предприятия.

Применение секретного ключа для цифровой подписи является надежным методом защиты информации. Поскольку даже, если злоумышленник получит значительное количество сообщений с цифровой подписью, он не сможет, используя их вычислить подлинность за выделенный промежуток времени.

Однако, если злоумышленник вошел в доверие абонента, то получая данные о шифровании подписей, приходящих от абонента, он может их использовать для передачи другим абонентам. Для исключения данной

ситуации необходимо использовать правило подписи только контрольной суммы сообщения, даже если оно имеет незначительный размер.

Шифр представляет собой систему преобразования текста с секретным ключом, что позволяет обеспечить секретность передаваемых информационных данных. Наиболее важным параметром шифра является ключ, представленный в виде криптографического алгоритма, позволяющего обеспечить выбор одного из преобразований информационных данных.

К методам криптографического преобразования информации применяют следующие требования:

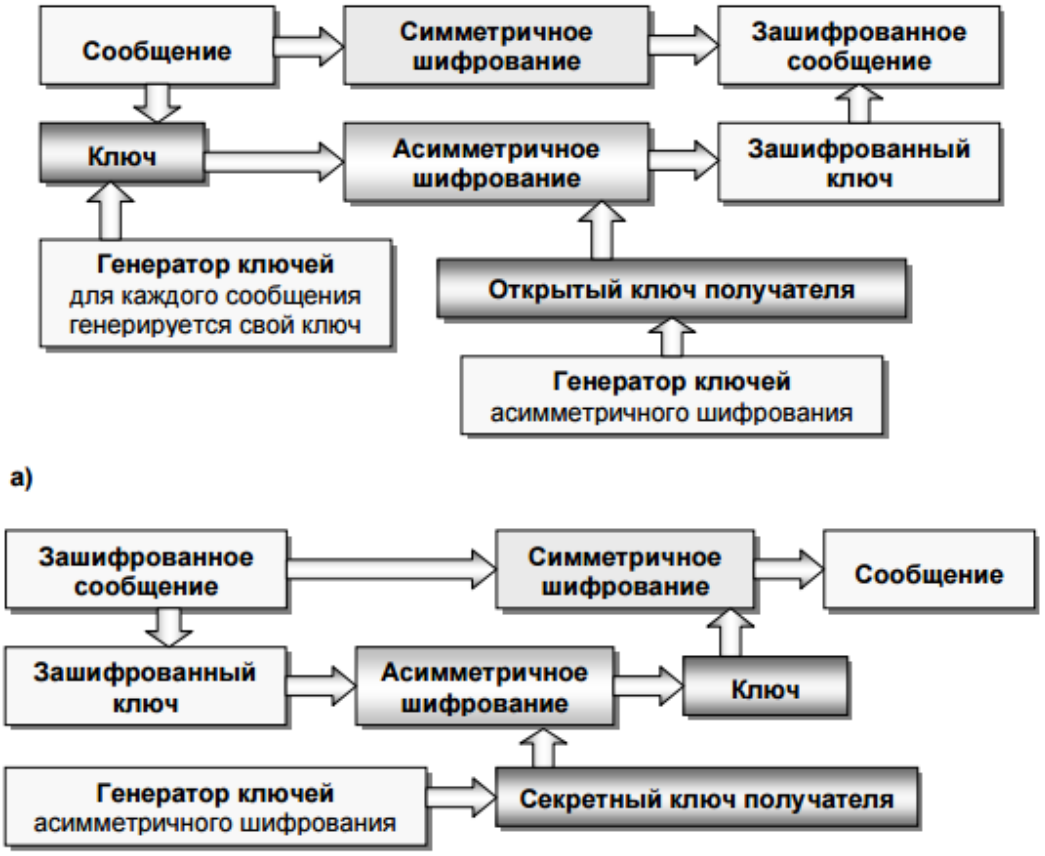
- выбранный метод преобразования информации должен обладать устойчивостью к попыткам получения исходного кода текста на основе зашифрованных данных;
- используемый ключ шифрования, не должен быть громоздким и трудным для запоминания;
- затраты, выделенные на шифрование данных должны быть оптимальными для обеспечения требуемого уровня защиты информации;
- возникающие ошибки в шифровании данных, не должны создавать потерю информации;
- длина зашифрованного информационного сообщения не должна превышать длину исходного кода.

Криптосистемы подразделяются на:

1) симметричные системы, основанные на использовании одного и того же ключа защиты данных в операциях шифрования и дешифрования данных

2) асимметричные системы, в которых ключ шифрования, отличается от ключа расшифрования. При этом, даже получив информацию об открытом ключе, злоумышленник не сможет определить секретный ключ.

Методы, позволяющие осуществить эффективное шифрование и дешифрование данных, приведены на рисунке 2.6.



a) эффективное шифрование сообщения;
b) дешифрования эффективно зашифрованного сообщения.

Рисунок 2.6 – Методы, позволяющие осуществить эффективное шифрование и дешифрование данных

На рисунке 2.6 мы можем проследить, как происходит шифрование сообщения и дешифровка. Здесь изображены все стадии прохождения шифрования сообщения при обоих вариантах шифрования сообщения. Имея исходное сообщение с помощью специального ПО, мы генерируем ключ шифрования для данного сообщения, после чего программа генерирует открытый ключ получателя, затем сообщение зашифровывается. При дешифровке данного сообщения получатель с помощью открытого ключа через тоже ПО формирует секретный ключ получателя, после чего программа расшифровывает сообщение. Но наиболее эффективным является метод ассиметричного шифрования.

Достоинствами аппаратных методов криптографических функций защиты данных являются:

- возможность обеспечения целостности данных при реализации алгоритма криптозащиты;
- шифрование и хранение ключей в плате аппаратного обеспечения, а не в оперативной памяти компьютера;
- создание системы защиты информации от несанкционированного доступа к информации.

Следует отметить, что криптографические механизмы применяют для управления идентичностью, реализации технологии доверенной платформы, разграничения доступа, управления авторством, построения сетей VPN. В отличие от других методов они позволяют обеспечить гарантирование уничтожение данных и обеспечить высокий уровень защиты от физической кражи носителя информации.

Применение технологии управления идентичностью, основанной на криптозащиты, позволяет поддерживать систему цифровых сертификатов, обеспечить высокий уровень контроля защиты данных с помощью цифровых удостоверений. Многие организации внедряют данную технологию для замены метода, основанного на паролях, что позволяет повысить доверие пользователей к выбранным ресурсам.

Технология разграничения доступом применяется фактически в любой системе защиты информации. Основной целью внедрения данной технологии организация многопользовательского доступа к защищенной информации на основании использования принципов назначения ролей, привилегий и защиты каждой группы пользователей с использованием криптозащиты.

Технология доверенных платформенных модулей (TPM) используется для реализации аппаратных функций, обеспечивающих необходимый уровень защиты данных. Для реализации данной технологии применяют микросхему, оснащенную механизмами физической безопасности от подделки данных и защиты от вредоносного программного обеспечения.

- возможность создания, хранения и ограничение использования ключей шифрования;

- обеспечить необходимый уровень целостности данных.

Среди достоинств криптографических методов защиты следует отметить высокий уровень защиты данных, экономичность в реализации и эффективность в быстродействии.

Недостатком криптографических методов защиты является сложность в реализации, что требует привлечение специалистов по криптографии для обеспечения требуемого уровня защиты данных.

Криптографические методы защиты информации относятся к программному комплексу защиты информации, но в тенденциях современного бизнеса это направление защиты информации становится все актуальнее. Так как вся отчетность и многие торговые операции в связи с улучшением информационных технологий переходят на электронный документооборот, и подлинность документов и подписей необходимо подтверждать, а также защищать документы от правки или доступа к ним посторонних лиц то криптография как метод защиты информации на мой взгляд является отдельным методом в политике информационной безопасности. И криптографические методы защиты информации являются очень эффективными.

Во второй главе выпускной квалификационной работы приведена характеристика организационных, программно-аппаратных, криптографических методов и средств защиты и на основании этого получены следующие авторские выводы:

- организационные меры обеспечения политики информационной безопасности предприятия - регламентируют документально использование мер информационной защиты, что регламентирует работу всей политики информационной безопасности;
- аппаратные и программные средства обеспечения информационной безопасности в строительной компании очень эффективны в комплексе что дает наибольшую защиту данных и более соответствует необходимым нормам

политики информационной безопасности;

− в настоящее время среди криптографических методов и средств, используемых на предприятия, наиболее эффективными является криптографический метод защиты создания цифровой или электронной подписи.

Полученные результаты и сформулированные выводы позволяют перейти к рассмотрению материала третьей главы, посвященной разработке и внедрению рекомендаций для повышения информационной безопасности предприятия.

Глава 3 ОБОСНОВАНИЕ ЭКОНОМИЧЕСКОЙ ЭФФЕКТИВНОСТИ РЕАЛИЗАЦИИ ПОЛИТИКИ ИНФОРМАЦИОННОЙ БЕЗОПАСНОСТИ СТРОИТЕЛЬНОЙ ОРГАНИЗАЦИИ

3.1Выбор и обоснование методики расчёта экономической эффективности

Исходной посылкой экономической эффективности является очевидное предположение: с одной стороны, при нарушении защищенности информации наносится некоторый ущерб, с другой - обеспечение защитыинформации сопряжено с расходованием средств. Полная ожидаемая стоимость защиты может быть выражена суммой расходов на защиту и потерь от ее нарушения.

Очевидно, что оптимальным решением было бы выделение на защиту информации средств, минимизирующих общую стоимость работ по защите информации.

Также очевидно, что экономическая эффективность мероприятий по защите информации может быть определена, через объем предотвращенного ущерба или величину снижения риска для информационных активов организации.

Поскольку оптимальное решение вопроса о целесообразном уровне затрат на защиту состоит в том, что этот уровень должен быть равен уровню ожидаемых потерь при нарушении защищенности**,** достаточно определить только уровень потерь. В качестве одной из методик определения уровня затрат возможно использование следующей эмпирической зависимости ожидаемых потерь (рисков) от i-й угрозы информации [37]:

$$Ri = 10^{\,Si+Vi-4} \quad (1)$$

где S_i - коэффициент, характеризующий возможную частоту возникновения соответствующей угрозы;

V_i - коэффициент, характеризующий значение возможного ущерба при ее возникновении. Si и Vi, приведены в таблице 3.1.

Таблица 3.1 – Значения коэффициентов S_i и V_i

Ожидаемая (возможная)частота появления угрозы	***Предполагаемое значение S_i***
Почти никогда	0
1 раз в 1 000 лет	1
1 раз в 100 лет	2
1 раз в 10 лет	3
1 раз в год	4
1 раз в месяц (примерно, 10 раз в год)	5
1-2 раза в неделю (примерно 100 раз в год)	6
3 раза в день (1000 раз в год)	7
Значение возможного ущерба при проявлении угрозы, руб.	***Предполагаемое значение Vi***
30	0
300	1
3 000	2
30 000	3
300 000	4
3 000 000	5
30 000 000	6
300 000 000	7

Суммарная стоимость потерь определяется формулой:

$$R = \sum_{i=1}^{N} Ri \qquad (2)$$

где N – количество угроз информационным активам, определенных в п.1.2.3.

При расчете суммарного показателя рекомендуется принять, что угрозы конфиденциальности, целостности и доступности реализуются нарушителем независимо. То есть, если в результате действий нарушителя была нарушена целостность информации, предполагается, что её содержание по-прежнему остается ему неизвестным (конфиденциальность не нарушена), а авторизованные пользователи по-прежнему имеют доступ к активам, пусть и искаженным (см. таблицу 3.2).

Таблица 3.2 -Величины потерь (рисков) для критичных информационных ресурсов до внедрения/модернизации защиты информации

Актив	***Угроза***	***Величина потерь (тыс.руб.)***
Проектная документация, разработанная организацией	конфиденциальности	100
Проектная документация, разработанная организацией	целостности	500
Проектная документация, разработанная организацией	доступности	20
Проектная документация, полученная от заказчика	конфиденциальности	100
Проектная документация, полученная от заказчика	целостности	100
Проектная документация, полученная от заказчика	доступности	20
Проектная документация, планы коммуникаций в т.ч. стратегического назначения.	конфиденциальности	500
Проектная документация, планы коммуникаций в т.ч. стратегического назначения.	целостности	100
Проектная документация, планы коммуникаций в т.ч. стратегического назначения.	доступности	20
Личные данные клиента	конфиденциальности	300
Личные данные клиента	целостности	20
Личные данные клиента	доступности	20
Личные сведения о сотрудниках	конфиденциальности	100
Личные сведения о сотрудниках	целостности	10
Личные сведения о сотрудниках	доступности	10
Системное программное обеспечение	конфиденциальности	0
Системное программное обеспечение	целостности	100
Системное программное обеспечение	доступности	100
Прикладное программное обеспечение (в т.ч. САПР, CMS, ERP, CRM и т.д.)	конфиденциальности	0

Продолжение таблицы 3.2

Прикладное программное обеспечение (в т.ч. САПР, CMS, ERP, CRM и т.д.)	целостности	100
Прикладное программное обеспечение (в т.ч. САПР, CMS, ERP, CRM и т.д.)	доступности	100
Суммарная величина потерь		2320

После произведения расчетов и построения таблицы 3.2 мы определились с риском финансовых потерь для предприятия, которая может составить приблизительно 2 320 000 рублей. Из этого можно сделать вывод, что для предприятия это будет очень существенной потерей. Для понятия насколько эффективна заработанная политика информационной безопасности необходимо произвести расчет показателей экономической эффективности проекта

3.2 Расчёт показателей экономической эффективности проекта

Риск владельца информации зависит от уровня инженерно-технической защиты информации, который, в свою очередь, определяется ресурсами системы.

Ресурс может быть определен в виде количества людей, привлекаемых к защите информации, в виде инженерных конструкций и технических средств, применяемых для защиты, денежных сумм для оплаты труда людей, строительства, разработки и покупки технических средств, их эксплуатации и других расходов. Наиболее общей формой представления ресурса является денежная мера. Ресурс, выделяемый на защиту информации, может иметь разовый и постоянный характер.

Разовый ресурс расходуется на закупку, установку и наладку дорогостоящей техники.

Постоянный ресурс - на заработную плату сотрудникам службы безопасности и поддержание определенного уровня безопасности, прежде

всего, путем эксплуатации технических средств и контроля эффективности защиты.

Таким образом, для определения экономической эффективности защиты информации предприятия необходимы следующие данные (показатели):

- расходы (выделенные ресурсы) на создание/модернизацию данной и поддержание её в работоспособном состоянии;
- величины потерь (рисков), обусловленных угрозами информационным активам после внедрения/модернизации защиты информации.

Данные о содержании и объеме разового ресурса, выделяемого на защиту информации, представлены в приложении Б в таблице 3.3 [37].

Содержание и объем постоянного ресурса, выделяемого на защиту информации, представлены в таблице 3.4.

Таблица 3.4 - Содержание и объем постоянного ресурса, выделяемого на защиту информации

Организационные мероприятия				
№ п\п	Выполняемые действия	Среднечасовая зарплата специалиста (руб.)	Трудоемкость операции (чел.час.)	Стоимость, всего (тыс.руб.)
1.	Проведение тренингов, инструктажей.	0,3	10	3
Стоимость проведения организационных мероприятий, всего				3
Мероприятия инженерно-технической защиты				
№ п/п	Номенклатура ПиАСИБ, расходных материалов	Стоимость, единицы (тыс.руб.)	Кол-во (ед.измерения)	Стоимость, всего (тыс.руб.)
2.	Обновление ПО	15	1	15
3.	Обслуживание видеонаблюдения	0,3	10	3

Продолжение таблицы 3.4

4.	Обслуживание детекторов движения	0,3	10	3
5.	Обслуживание противопожарной системы	0,3	20	6
Стоимость проведения мероприятий инженерно-технической защиты				27

Таким образом, для разработки информационной безопасности требуется 355 640 руб., а для ежегодной поддержки - 30 000 руб.

Для проведения расчета необходимо получить прогнозируемые данные о величине потерь (рисков) для критичных информационных ресурсов после внедрения/модернизации защиты информации. Результаты формируются по результатам экспертного опроса (см. таблицу 3.5).

Таблица 3.5 - Величины потерь (рисков) для критичных информационных ресурсов после внедрения/модернизации защиты информации

Актив	***Угроза***	***Величина потерь (тыс.руб.)***
Проектная документация, разработанная организацией	конфиденциальности	10
Проектная документация, разработанная организацией	целостности	50
Проектная документация, разработанная организацией	доступности	2
Проектная документация, полученная от заказчика	конфиденциальности	10
Проектная документация, полученная от заказчика	целостности	10
Проектная документация, полученная от заказчика	доступности	2
Проектная документация, планы коммуникаций в т.ч. стратегического назначения.	конфиденциальности	50
Проектная документация, планы коммуникаций в т.ч. стратегического назначения.	целостности	10

Продолжение таблицы 3.5

Актив	***Угроза***	***Величина потерь (тыс.руб.)***
Проектная документация, планы коммуникаций в т.ч. стратегического назначения.	доступности	20
Личные данные клиента	конфиденциальности	30
Личные данные клиента	целостности	2
Личные данные клиента	доступности	2
Личные сведения о сотрудниках	конфиденциальности	10
Личные сведения о сотрудниках	целостности	1
Личные сведения о сотрудниках	доступности	1
Системное программное обеспечение	конфиденциальности	0
Системное программное обеспечение	целостности	10
Системное программное обеспечение	доступности	10
Прикладное программное обеспечение (вт.ч. САПР, CMS, ERP, CRM и т.д.)	конфиденциальности	0
Прикладное программное обеспечение (в т.ч. САПР, CMS, ERP, CRM и т.д.)	целостности	10
Прикладное программное обеспечение (в т.ч. САПР, CMS, ERP, CRM и т.д.)	доступности	10
Суммарная величина потерь		232

Оценка динамики величин потерь за период 2года (см. таблицу 3.6)

Таблица 3.6 - Оценка динамики величин потерь

	1 кв.	2 кв.	3 кв.	1 год	1 кв.	2 кв.	3 кв.	2 год
До внедрения СЗИ	580	1160	1740	2320	2900	3480	4060	4640
После внедрения СЗИ	58	116	174	232	290	348	406	464
Снижение потерь	522	1044	1566	2088	2610	3132	3654	4176

После принятия обязательных допущений о неизменности частоты появления угроз, а также о неизменном уровне надежности созданной защиты

информации, возможно определить срок окупаемости ($T_{ок}$). Это выполняется аналитическим способом, с использованием приведенной ниже формулы:

$$T_{ок} = \frac{R_{\Sigma}}{(R_{ср} - R_{прогн})} \quad (3)$$

и графическим, как это представлено на рисунке 3.1.

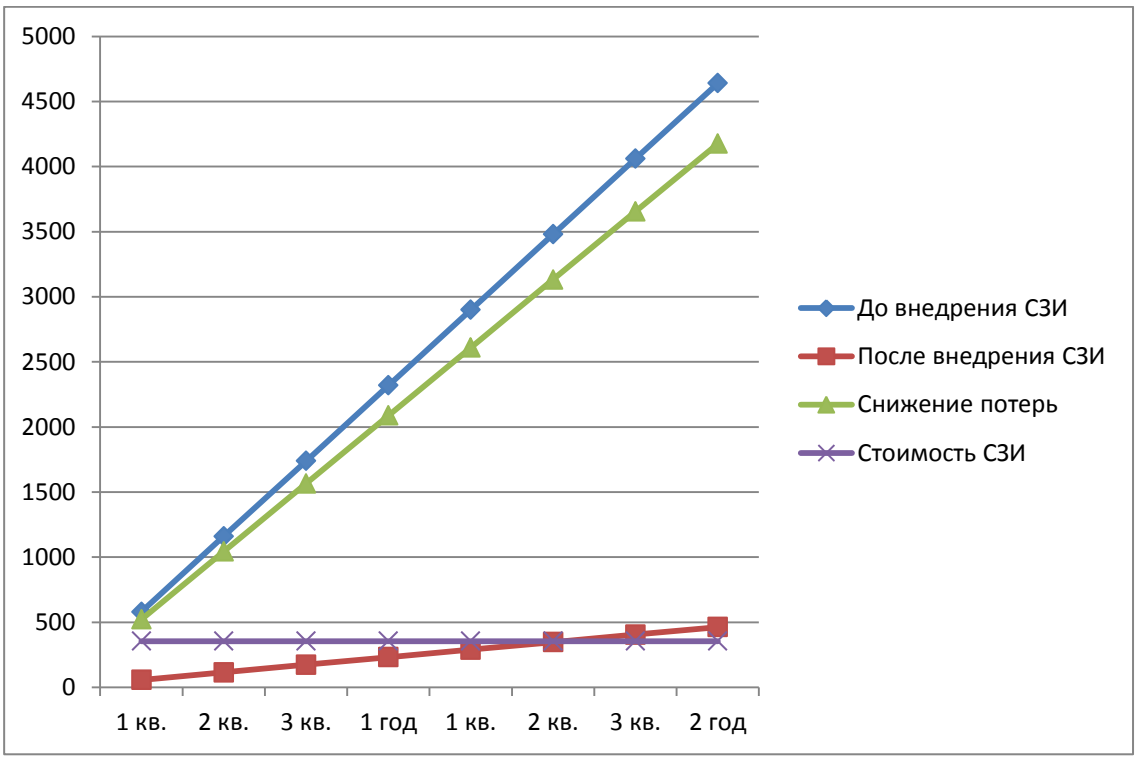


Рисунок 3.1 - Графическое определение срока окупаемости

Таким образом экономические расчеты показывают эффективность внедрения комплекса информационной защиты. Согласно проведённым расчётам, окупаемость информационной безопасности произойдёт ещё в первом квартале её использования. Что для предприятия является очень минимальной финансовой нагрузкой.

В данной главе произведены расчеты, из них мы можем увидеть, что прогнозируемый ущерб является достаточно весомым для предприятия, а едино разовые затраты на реализацию политики информационной безопасности меньше, чем предполагаемые финансовый ущерб. Это говорит о том, что реализация политики информационной безопасности поможет защитить

данные, и это будет эффективная защита, которая поможет предотвратить финансовые потери для компании от возможных угроз. И через 2 года политика информационной безопасности, реализованная в компании, поможет защитить порядка четырех миллионов рублей. Соответственно можно сделать вывод, что разработанная политика информационной безопасности является очень эффективной.

ЗАКЛЮЧЕНИЕ

В процессе выполнения выпускной квалификационной работы была разработана политика информационной безопасности предприятия.

На основании анализа основных положений теории защиты информации было установлено, что для создания политики информационной безопасности необходимо разработать целый ряд документов и инструкций, направленных на защиту информации. И ни в коем случае нельзя останавливаться на одном методе защиты информации, иначе защита данных будет под угрозой. Защита данных должна быть комплексной. Комплексная политика информационной безопасности включает в себя разработку, производство и установку технических средств защиты, а также регулярное проведение проверок используемого информационного оборудования. В настоящее время на многих предприятиях разворачивается работа по аттестации информатизированных объектов на предмет соответствия их требованиям информационной безопасности.

Одно из направлений развития современных предприятий — информатизация. Использование современных информационных технологий позволяет существенно повысить эффективность производственных и управленческих процессов. Но вместе с применением этих технологий возникает проблема обеспечения комплексной защиты информации, которая может быть отнесена к конфиденциальной.

В рамках данного проекта была разработана комплексная система защиты информации на предприятии. Разработка данного проекта заключалась в следующем:

- выявление недостатков действующей информационной защиты предприятия;
- выявление типов угроз, могущих возникнуть в результате наличия недостатков в защите информационных систем предприятия;
- выбор методов и способов решения существующих проблем.

В качестве решения был разработан комплекс мер, который состоит из:

− административных решений, которые регулируют возможности утечки информации в результате влияния человеческого фактора;

− программно-аппаратных решений, которые позволили минимизировать риск возникновения атаки на информационные каналы из внешней среды или с применением различных устройств хранения информации;

− инженерно-технических решений, которые позволят предотвратить порчу или хищение различных хранилищ информации, минимизировать риск возникновения атаки на информационные каналы из внешней среды или с применением различных устройств хранения информации, либо порчу их в результате различных форс - мажорных обстоятельств.

На основании анализа основных методов и средств защиты информации было установлено, что организационно-правовые методы и средства защиты информации должны быть направлены на противодействие угрозам информационной безопасности, снижать риски и эффективно обрабатывать инциденты с целью длительного обеспечения достаточного уровня защиты данных.

Инженерно-технические методы защиты информации, основаны на защите информации на контролируемой территории, внутри помещений, сети, программном обеспечении и имеющихся баз данных.

Аппаратно-программные методы защиты направлены на обеспечение сетевой безопасности на сетевом, пользовательском уровнях, в том числе и на уровне приложений.

В настоящее время среди криптографических методов и средств, используемых на предприятия, наиболее эффективным является криптографический метод создания цифровой или электронной подписи.

На основании выполненного анализа наиболее эффективными методами и средствами защиты информации является комплекс мер как инженерно-технических методов и средств, позволяющих обеспечить комплексную защиту данных на предприятии, так и аппаратно-программных, и криптографических.

Политика информационной безопасности разработана и её эффективность доказана. Оценка эффективности предложенных мероприятий показала их целесообразность внедрения в организации. В конце проекта было дано экономическое обоснование эффективности и окупаемости защиты информации, в результате которой было установлено, что окупаемость защиты происходит за несколько лет, причём время окупаемости прямо пропорционально количеству отраженных атак, а эффективность будет расти с каждым годом.

Учитывая, что все поставленные задачи полностью решены, можно обоснованно утверждать, что главная цель исследования – достигнута.

СПИСОК ИСПОЛЬЗУЕМОЙ ЛИТЕРАТУРЫ

1. Национальный стандарт РФ «Защита информации. Основные термины и определения» (ГОСТ Р 50922-2006).
2. Национальный стандарт РФ «Информационная технология. Практические правила управления информационной безопасностью» (ГОСТ Р ИСО/МЭК 17799—2005)
3. Безопасность: теория, парадигма, концепция, культура. Словарь-справочник / Автор-сост. профессор В. Ф. Пилипенко. 2-е изд., доп. и перераб. — М.: ПЕР СЭ-Пресс, 2005.
4. Информационная безопасность (2-я книга социально-политического проекта «Актуальные проблемы безопасности социума»). М.: «Оружие и технологии», 2009.
5. Национальный стандарт РФ «Методы и средства обеспечения безопасности. Часть 1. Концепция и модели менеджмента безопасности информационных и телекоммуникационных технологий» (ГОСТ Р ИСО/МЭК 13335-1 — 2006)
6. Рекомендации по стандартизации «Информационные технологии. Основные термины и определения в области технической защиты информации» (Р 50.1.053-2005
7. Рекомендации по стандартизации «Техническая защита информации. Основные термины и определения» (Р 50.1.056-2005)
8. Государственный стандарт РФ «Аспекты безопасности. Правила включения в стандарты» (ГОСТ Р 51898-2002)
9. Бабаш А.В. История криптографии. Ч. 1 / А. В. Бабаш, Г. Н. Шанкин. - М. : Гелиос АРВ, 2012. - 240 с.
10. Панкратов Ф.Г. Коммерческая деятельность : учеб.для вузов / Ф. Г. Панкратов. - Изд. 8-е, перераб. и доп. - М. : Дашков и Ко, 2015. - 502 с.
11. Экономика защиты информации : метод.указания к экономической части диплом. проектов для студентов очной формы обучения специальности

090103 "Организация и технология защиты информации" / Брян. гос. техн. ун-т ; [разраб. М. Ф. Дриго]. - Брянск : Изд-во БГТУ, 2007. - 16 с.

12. Расторгуев С.П. Основы информационной безопасности : учеб.пособиедля вузов / С. П. Расторгуев. - М. :Academia, 2010. - 186 с.

13. Хаулет, Т. Защитные средства с открытыми исходными текстами = OPEN SOURCE SECURITY TOOLS : практ. рук. по защитным приложениям : учеб. пособие / Т. Хаулет ; пер. с англ. В. Галатенко и О. Труфанова под ред В. Галатенко. - М. : Интернет-Ун-т Информ. Технологий : БИНОМ.лаб. знаний, 2013. - 607 с.

14. Мельников В.П. Информационная безопасность и защита информации : учеб.пособиедля вузов / В. П. Мельников, С. А. Клейменов, А. М. Петраков ; под ред. С. А. Клейменова. - 2-е изд., стер. - М. :Academia, 2014. - 330 с. -

15. Саак, А.Э. Информационные технологии управления : учеб.для вузов / А. Э. Саак, Е. В. Пахомов, В. Н. Тюшняков. - 2-е изд. - М. [и др.] : Питер, 2013. - 318 с. + 1 электрон. опт. диск (CD-ROM) ;

16. Куприянов, А.И. Основы защиты информации : учеб.пособие/ А. И. Куприянов, А. В. Сахаров, В. А. Шевцов. - 3-е изд., стер. - М. :Academia, 2008. - 256 с.

17. Краковский, Ю.М. Информационная безопасность и защита информации : учеб.пособие/ Ю. М. Краковский. - М. ; Ростов н/Д : МарТ, 2008. - 287 с.

18. Баричев С.Г, Серов Р.Е. Основы современной криптографии: Учебное пособие. - М.: Горячая линия - Телеком, 2008.

19. Адигеев М.Г. Введение в криптографию. Часть 1. Основные понятия, задачи и методы криптографии. - Ростов-на-Дону: Изд-во РГУ, 2002. - 35 с.

20. БудкоВ.Н. Информационная безопасность и защита информации: Конспект лекций. - Воронеж: Изд-во ВГУ, 2013. - 86 с.

21. Варлатая С.К., Шаханова М.В. Аппаратно-программные средства и методы защиты информации: Учебное пособие. - Владивосток: Изд-во ДВГТУ, 2007. - 318 с.

22. ГрушоА.А., Тимонина Е.Е. Теоретические основы защиты информации. - М.: Изд-во "Яхтсмен", 1996. - 187 с.

23. Железняк В.К. Защита информации от утечки по техническим каналам: Учебное пособие. - СПб.: ГУАП, 2006. - 188 с.

24. Зубов А.Ю. Совершенные шифры. - М.: Гелиос АРВ, 2003. - 160 с.,

25. Казарин О.В. Безопасность программного обеспечения компьютерных систем. - М.: МГУЛ, 2013. - 212 с.

26. Мордвинов В.А., Фомина А.Б. Защита информации и информационная безопасность. - М.: МГДД(Ю)Т, МИРЭА, ГНИИ ИТТ "Информика", 2010. - 69 с.

27. Пазизин С.В. Основы защиты информации в компьютерных системах (учебное пособие). - М.: ТВП/ОПиПМ, 2003. - 178 с.

28. РжавскийК.В. Информационная безопасность: практическая защита информационных технологий и телекоммуникационных систем: Учебное пособие. - Волгоград: Изд-во ВолГУ, 2002. - 122 с.

29. Яковлев А.В., Безбогов А.А., Родин В.В., Шамкин В.Н. Криптографическая защита информации: Учебное пособие. - Тамбов: Издательство ТГТУ, 2006. - 140 с.

30. Беломойцев Д. А. Основные методы криптографической обработки данных: учеб. пособие / Д. А. Беломойцев, Т. М. Волосатов, С. В. Родионов. – М.: Московский государственный технический университет им. Н. Э. Баумана, 2014. – 80 с

31. Статья Программно - аппаратный комплекс - https://ru.wikipedia.org/wiki/Программно-аппаратный_комплекс [Электронный ресурс]

32. Политика информационной безопасности (финансовые организации) Материал из

SecurityPolicy.ru http://w15408.narod.ru/docs/Policy_itsec_fin.doc[Электронный ресурс]

33. Информационная безопасность в ГУП ОЦ "Московский дом книги"Вид работы: диплом http://bibliofond.ru/view.aspx?id=513939#1 [электронный ресурс]

34. Павлова Тема 11 Современные технологии защиты информации http://window.edu.ru/resource/432/57432/files/pavlova.zip[электронный ресурс]

35. 090103.65 Организация и технология защиты информации июнь 2012документ PDF http://belca.islu.ru[электронный ресурс]

36. Козлов В.Е. К вопросу об инженерно-техническом обеспечении компьютерной безопасности: Научная статья

37. Выбор и обоснование методики расчёта экономической эффективности http://zdamsam.ru/a72347.html[электронный ресурс]

ПРИЛОЖЕНИЕА

Таблица 1.2 - Результаты оценки уязвимости активов

Группа уязвимостей Содержание уязвимости	Прикладное программное обеспечение (в т.ч. САПР, CMS, ERP, CRM и т.д.)	Системное программное обеспечение	Личные сведения о сотрудниках	Личные данные клиента	Проектная документация, планы коммуникаций в т.ч. стратегического назначения.	Проектная документация, полученная от заказчика	Проектная документация, разработанная организацией
1. Среда и инфраструктура							
Действия злоумышленников	Высокая	Высокая					
2. Аппаратное обеспечение							
Выход из строя АО	Высокая	Высокая					Высокая
Недостача ресурсов АО	Высокая	Низкая					
3. Программное обеспечение							
Конструктивные недостатки ПО	Высокая	Высокая					
Выход из строя ПО	Высокая	Высокая					

Продолжение таблицы1.2

Недостача ресурсов ПО	Высокая	Высокая					
Группа уязвимостей Содержание уязвимости	Прикладное программное обеспечение (в т.ч. САПР, CMS, ERP, CRM и т.д.)	Системное программное обеспечение	Личные сведения о сотрудниках	Личные данные клиента	Проектная документация, планы коммуникаций в т.ч. стратегического назначения.	Проектная документация, полученная от заказчика	Проектная документация, разработанная организацией
4. Коммуникации							
Похищение при передаче по ЛС						Высокая	Высокая
Подмена при передаче по ЛС						Низкая	Низкая
Отказ в облуживании ЛС						Низкая	Низкая
5. Документы (документооборот)							
Ошибки пользователя			Низкая	Низкая			

Продолжение таблицы1.2

Группа уязвимостей Содержание уязвимости	Прикладное программное обеспечение (в т.ч. САПР, CMS, ERP, CRM и т.д.)	Системное программное обеспечение	Личные сведения о сотрудниках	Личные данные клиента	Проектная документация, планы коммуникаций в т.ч. стратегического назначения.	Проектная документация, полученная от заказчика	Проектная документация, разработанная организацией
6.Персонал							
Разглашение конфиденциальной информации			Высокая	Высокая	Высокая	Высокая	Высокая
Халатное отношение к информационной безопасности			Высокая	Высокая	Высокая	Высокая	Высокая
Саботаж							Низкая
7. Общие уязвимые места							
Возникновение ЧС							Высокая
Обстоятельства непреодолимой силы							Высокая

ПРИЛОЖЕНИЕ Б

Таблица 3.3 - Содержание и объем разового ресурса, выделяемого на защиту информации

Организационные мероприятия				
№ п\п	Выполняемые действия	Среднечасовая зарплата специалиста (руб.)	Трудоемкость операции (чел.час.)	Стоимость, всего (тыс.руб.)
1	Разработка методик и приказов	220	5	1100
2	Доведение информации до сотрудников, обучение, тренинги.	220	2	440
Стоимость проведения организационных мероприятий, всего				1540
Мероприятия инженерно-технической защиты				
№ п/п	Номенклатура ПиАСИБ, расходных материалов	Стоимость, единицы (тыс.руб.)	Кол-во (ед.измерения)	Стоимость, всего (тыс.руб.)
1	Лицензионная версия TrafficQuota	3	1	3,0
2	Лицензионная версия TrafficInspector	3,5	1	3,5
3	Лицензионная версия ISA Server	5,2	1	5,2
4	Приобретение лицензии на антивирусную систему (комплексное решение в комплекте с антиспам, фаервол, защита эл. почты и т.д.)	2	16	32
5	Лицензии на ОС Windows10 с возможностью даунгрейда до 7.	9,2	16	147,2
6	Установка и обновление программного обеспечения чел./час.	0,3	40	12
7	Пломбы и инструменты опломбировки	12	1	12
8	Опломбировка чел./час.	0,3	8	2,4
9	Запорные приспособления	1	5	5
10	Монтаж запорных приспособлений	0,2	5	1

Продолжение таблицы 3.3

№ п/п	Номенклатура ПиАСИБ, расходных материалов	Стоимость, единицы (тыс.руб.)	Кол-во (ед.измерения)	Стоимость, всего (тыс.руб.)
11	Камеры видеонаблюдения	5,2	4	20,8
12	Провода, соединители, разъемы и т.п.	3,5	1	3,5
13	Система архивирования записи видеонаблюдения	7	1	7
14	Монтаж видеонаблюдения чел./час.	0,3	10	3
15	Детектор движения	1	11	11
16	Провода, соединители, разъемы и т.п.	3,5	1	3,5
17	Пульт контроля и оповещения	6	1	6
18	Монтаж детекторов движения чел./час.	0,3	12	3,6
19	Датчики задымления	0,8	26	20,8
20	Провода, соединители, разъемы и т.п.	3,5	1	3,5
21	Монтаж противопожарной систем оповещения	0,3	12	3,6
22	Средства ручного пожаротушения	0,5	10	5
23	Средств аавтоматического пожаротушения	30	1	30
24	Провода, соединители, разъемы и т.п.	3,5	1	3,5
25	Монтаж пожаротушения чел./час.	0,3	20	6
Стоимость проведения мероприятий инженерно-технической защиты				354,1