СОДЕРЖАНИЕ

ПЕРЕЧЕНЬ СОКРАЩЕНИЙ И УСЛОВНЫХ ОБОЗНАЧЕНИЙ.....7

ВВЕДЕНИЕ.....8

1 ТЕОРЕТИЧЕСКИЕ ОСНОВЫ РЕШАЕМОЙ ПРОБЛЕМЫ 11

1.1 Постановка задачи.....11

1.2 Основные угрозы информационной безопасности малых, средних и крупных предприятий.....11

1.3 Современные подходы к анализу существующих систем информационной безопасности предприятий.....20

1.4 Этапы процесса модернизации системы информационной безопасности предприятия.....24

2 ХАРАКТЕРИСТИКА ПРЕДПРИЯТИЯ.....31

2.1 Описание предприятия.....31

2.2 Построение модели угроз информационной безопасности предприятий.....32

2.3 Типовые проблемы существующих систем информационной безопасности и методы их решения.....38

2.4 Разработка концепции информационной безопасности.....42

2.5 Разработка политики информационной безопасности.....44

3 ПРОЕКТНАЯ ЧАСТЬ.....47

3.1 Разработка плана модернизации системы информационной безопасности.....47

3.2 Необходимое аппаратное обеспечение системы защиты информации.....49
3.3 Необходимое программное обеспечение системы защиты информации.....71
ЗАКЛЮЧЕНИЕ.....79
СПИСОК ИСПОЛЬЗОВАННЫХ ИСТОЧНИКОВ.....81

ПЕРЕЧЕНЬ СОКРАЩЕНИЙ И УСЛОВНЫХ ОБОЗНАЧЕНИЙ

АРМ – автоматизированное рабочее место;

ВКР – выпускная квалификационная работа;

ГОСТ – государственный отраслевой стандарт;

КСЗИ – комплексная система защиты информации;

НСД – несанкционированный доступ;

ОС – охранная сигнализация;

ОПС – охранно-пожарная сигнализация;

ПО – программное обеспечение;

ПС – пожарная сигнализация;

ПТБ – правила техники безопасности;

ПТЭ – правила технической эксплуатации;

ПУЭ – правила устройства электроустановок;

ПЭМИН – побочные электромагнитные излучения и наводки;

РД – руководящий документ;

СЗИ – система защиты информации;

СКУД – система контроля и управления доступом;

СОВ – системы обнаружения вторжений;

СПВ – системы предотвращения вторжений;

ТЗ – техническое задание;

ТО – техническое обслуживание;

ЭВМ – электронно-вычислительная машина.

ВВЕДЕНИЕ

Современный уровень информатизации экономики задает особые требования к хранению и распространению информации. Информация стала серьезным ресурсом, неправильное обращение с которым несет огромные финансовые, репутационные и правовые риски. Поэтому многие российские компании стараются решать задачи защиты информации глобально – путем создания системы информационной безопасности, отвечающей современным стандартам и требованиям целости, доступности и конфиденциальности. Если для «молодых» предприятий подобные системы можно выстраивать «с нуля», то для компаний, давно работающих на рынке, требуется провести более ресурсо- и трудоемкую процедуру модернизации.

Актуальность темы ВКР. Поскольку, как писалось выше, вопрос модернизации системы информационной безопасности на предприятиях стоит очень остро, требуется формализация и стандартизация процесса модернизации. Стандартизация позволит значительно уменьшить издержки и сократить время, затраченное на процесс модернизации. Для этой цели необходимо разработать четкую методологию. Именно поэтому тема «Разработка методологии системы информационной безопасности предприятия» является более чем актуальной.

Степень научной разработанности проблемы.Данный вопрос неоднократно поднимался в научной литературе [9, 20]. В ряде источников [16, 17, 18] рассмотреныразличные возможности моделирования систем

информационной безопасности, однако не найдено ни одной работы, в которой модернизация информационных систем была бы рассмотрена в комплексе.

Объект исследования: система информационной безопасности предприятия.

Предмет исследования: существующие механизмы защиты информации на предприятии.

Цель исследования: разработка методологии модернизации системы информационной безопасности предприятия.

Задачи исследования:

- анализ основных угроз информационной безопасности малых, средних и крупных предприятий;
- изучение современных подходов к анализу существующих систем информационной безопасности предприятий;
- описание этапов процесса анализа и модернизации системы информационной безопасности предприятия;
- построение универсальной модели угроз предприятий;
- подбор необходимого аппаратного обеспечения системы защиты информации;
- подбор необходимого программного обеспечения системы защиты информации;
- анализ типовых проблем существующих систем информационной безопасности и разработка методов их решения;
- разработка концепции информационной безопасности;

- разработка политики информационной безопасности
- разработка детальных политик безопасности.

Теоретическая и практическая значимость. Теоретическая значимость данной ВКР определяется вкладом в развитие методик и подходов к построению системы информационно безопасности предприятия с высокими показателями защищенности. Практическая значимость данной ВКР заключается в том, что разработанная методология позволит формировать на своей основе планы модернизации систем информационной безопасности конкретных предприятий.

Теоретико-методологические основы исследования. В качестве теоретико-методологических основ исследования в данной ВКР рассматривается целый ряд работ таких авторов как Ю.А. Родичев, К.Я. Мытник, А.В. Бабаш [33, 27, 4]. При решении поставленных задач использованы научно разработанные методы познания, проверенные на практике. В качестве основополагающих документов и стандартов используются национальные стандарты Российской Федерации (ГОСТы) и международные стандарты (ISO). Также рассмотрены законы Российской Федерации, постановления правительства РФ и иные нормативные акты и документы, относящиеся к вопросам защиты информации.

Структура выпускной квалификационной работы. Данная выпускная квалификационная работа состоит из введения, трех глав, заключения, списка литературы и приложений.

1 ТЕОРЕТИЧЕСКИЕ ОСНОВЫ РЕШАЕМОЙ ПРОБЛЕМЫ

1.1 Постановка задачи

Термин «методология» определяется толковым словарем как «система принципов и способов организации и построения теоретической и практической деятельности, а также учение об этой системе» [3]. В рамках данной квалификационной работы разрабатывается методология модернизации системы информационной безопасности предприятия. На основе данной методологии для каждого конкретного предприятия может быть построена технологическая карта.

1.2 Основные угрозы информационной безопасности малых, средних и крупных предприятий

Предприятиям любого размера в процессе своей деятельности приходится сталкиваться с различными угрозами информационной безопасности.

Источники угроз могут быть как внутренними, так и внешними. Можно выделить пять основных источников:

- злоумышленники, проникающие извне;
- вредоносные программы;
- сотрудники-злоумышленники (инсайдеры);
- сотрудники, нарушающие информационную безопасность неумышленно;
- стихийные бедствия.

Как правило, угрозы информационной безопасности проявляются в результате потенциального взаимодействия с самыми уязвимыми частями системы защиты предприятия, т.е. за счет факторов уязвимости [5].

Наиболее часто встречаются следующие факторы:

- ошибки в программном обеспечении;
- несовершенство аппаратного обеспечения;
- неполноценное функционирование процессов автоматизированных систем;
- неточность протоколов обмена информацией;
- сложные или нештатные условия эксплуатации систем.

Уязвимости делятся на три больших класса: объективные, случайные и субъективные [6].

Объективные уязвимости зависят от характеристик и технического построения оборудования на защищаемом предприятии. Полностью устранить уязвимости этого типа не представляется возможным, однако существует ряд средств, позволяющих снизить вероятность их эксплуатации. Объективные уязвимости делятся на четыре больших группы [16]:

1. Уязвимости, связанные с техническими средствами излучения. К этой группе относятся побочные электромагнитные излучения и сигналы от кабельных линий, акустические утечки, проскальзывание сигналов в цепочки электрического тока, наводки на линии и проводники.

2. Активизируемые уязвимости. Эта группа уязвимостей включает в себя вредоносное программное обеспечение и аппаратные закладки

3. Уязвимости, создаваемые особенностями защищаемого объекта. Как правило, подобные уязвимости связаны с расположением защищаемого объекта и организацией каналов обмена информацией.

4. Уязвимости, зависимые от особенностей элементов-носителей. Эта группа уязвимостейпроявляется в деталях, обладающих электроакустическими модификациями или подпадающими под действие электромагнитного поля.

Случайные уязвимости относятся к переменным факторам, зависящим от особенностей информационной среды и непредвиденных обстоятельств. Эти факторы сложно предсказуемы, но устранять их необходимо в максимально кратчайшие сроки. К случайным могут относиться следующие уязвимости [21]:

- сбои технических средств на разных уровнях работы с информацией;
- неисправности отдельных элементов системы;
- сбои программного обеспечения;
- неполадки в работе вспомогательного оборудования;
- повреждение коммуникаций зданий предприятий;
- неисправности в работе ограждающих устройств.

Субъективные уязвимости являются результатами некорректных действий сотрудников, отвечающих за разработку и внедрение систем хранения информации и ее защиты. В первую очередь, это ошибки и неточности на этапах загрузки программного обеспечения, его повседневного использования, а также на этапе управления информационными системами и технической аппаратурой. Помимо этого, к этому классу относятся нарушения режима

доступа к личным данным, нарушения работы системы во время работы с устройствами и данными [32].

Каждая найденная уязвимость требует учета, анализа и оценки. Для оценки уязвимости необходимо определить критерии опасности возникновения угрозы. Это процесс называют ранжированием. Как правило, определяют три основных критерия:

1. Доступность. Данный критерий определяет возможность источника угроз использовать уязвимость. В этот показатель могут входить как технические данные носителя информации, так и уровень компетенции лица, эксплуатирующего уязвимость.

2. Фатальность. Этот показатель определяется потенциальными последствиями созданной угрозы и восстановимости системы в результате угрозы.

3. Количество. Количественный критерий оценивает результат подсчета частей информационной системы, подверженных уязвимости.

Общие значение критериев рассчитываются как среднее арифметическое суммы показателей отдельных уязвимостей. Расчет степени опасности представлен в виде формулы (1).

$$К(О)=(КД*КФ*КК)/125 \quad (1),$$

где:

- К(О) – степень опасности;
- КД – коэффициент доступности;
- КФ – коэффициент фатальности;
- КК – количественный коэффициент.

Полноценный расчет степени опасности требует глубокого анализа защищаемой информационной системы,

оценки всех уязвимостей, составления информационной карты.

Целями атак на информационные системы предприятий могут быть:

- кража коммерческой информации;
- кража персональных данных;
- искажение хранящейся информации;
- полная или частичная остановка деятельности предприятия;
- нанесение урона репутации компании.

Защищаемая информация должна отвечать четырем основным принципам:

5. Целостность. Информация должна сохранять структуру и вид в процессе хранения и передачи. Изменять и удалять информацию может только легитимный пользователь, обладающий соответствующими правами доступа.

6. Конфиденциальность. Доступ к информации должен быть ограничен четко заданным кругом лиц (за исключением публичной информации).

7. Доступность. Информация должна предоставляться легитимным пользователям беспрепятственно и с минимальной задержкой.

8. Достоверность. Источник информации должен определяться и подтверждаться однозначным способом. Таким же способом должна подтверждаться и целостность информации.

Логическая цепочка преобразования информации представлена на рис. 1.1.

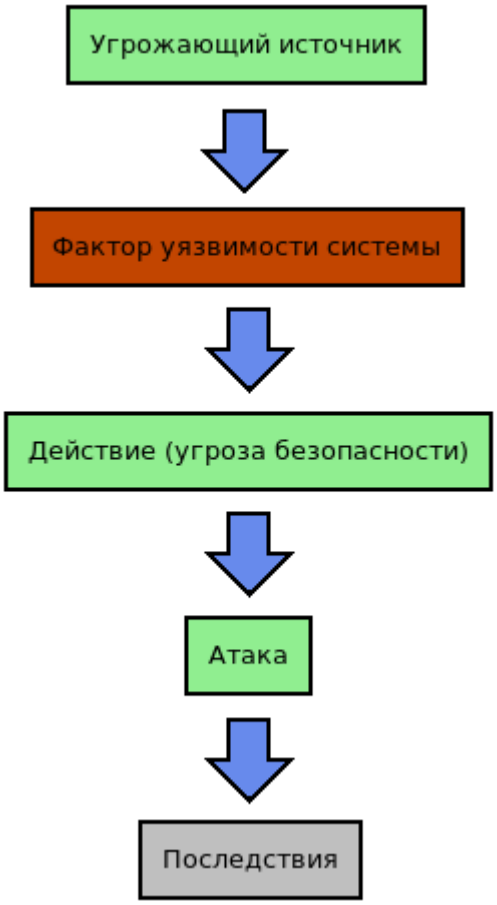

Рис. 1.1 – Логическая цепочка преобразования информации

Одной из мер обеспечения защиты от угроз является своевременное обращение в правоохранительные органы. Законодательство большинства развитых стран предполагают наказание за правонарушения в области нарушения информационной безопасности. Степень суровости наказания зависит от причиненного ущерба и типа объекта атаки. На рисунке 1.2 представлена география кибератак в 2019 году по данным Лаборатории Касперского [36].

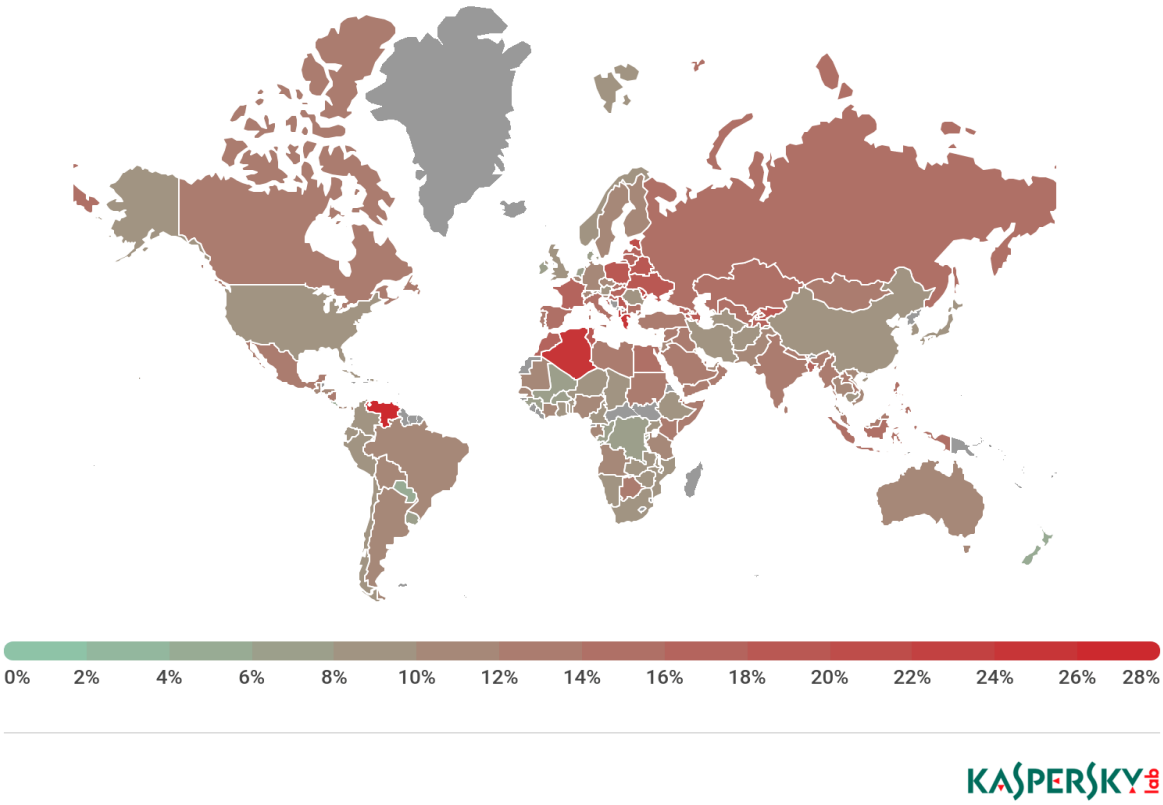

Рис. 1.2 – География кибератак за 2019 год

Статистически наиболее часто [37, 39] используются следующие типы атак информационных систем предприятий:

1. Удаленное проникновение. Этот тип атак позволяет осуществлять несанкционированное удаленное управление компьютера пользователя информационной системы из-за пределов локальной сети предприятия. Как правило, для удаленного проникновения либо эксплуатируются уязвимости операционной системы, либо используются методы социальной инженерии для воздействия на пользователя. Для борьбы с такими атаками необходимо, с одной стороны, разработать и применить в организации четкие политики обновлений и безопасности рабочих станций пользователей, а с другой – в обязательном порядке

проводить с сотрудниками обучающие семинары на тему информационной безопасности и принципов работы социальной инженерии.

2. Локальное проникновение. Данный тип атак похож на предыдущий, за исключением того, что осуществляется инсайдером из локальной сети предприятия. Часто благоприятной почвой для подобных атак является недостаточно жесткая политика сетевых экранов внутри локальной сети. Бороться с такими атаками позволяет сегментирование локальной сети, продуманные политики паролей и сетевых экранов.

3. Удаленная атака типа «отказ в обслуживании». Подобные атаки способны нарушить функционирование информационной системы или общедоступного ресурса. Этот тип атак является самым распространенным и технически самым примитивным. На рисунке 1.3 приведена статистика DDOS-атак по отраслям за 2019 год [36]. Часто DDOS-атаки производятся при помощи сети из зараженных компьютеров (так называемых «ботнетов»), владельцы которых могут даже не подозревать об этом. Компьютеры ботнета массово отправляют запросы к информационному ресурсу компании, нагружая каналы связи, программные и аппаратные ресурсы. Универсального метода борьбы с таким типом атак не существует. Если это экономически целесообразно, можно приобрести аппаратно-программный комплекс для борьбы с DDOS-атаками от компании Cisco, однако и он не будет являться панацеей. Наиболее разумный вариант – использовать специальные сервисы от компаний (Cloudflare, Incspsula, QRator, Akamai, Cloudbric), специализирующихся именно на этом виде атак. Все запросы от пользователей

первоначально направляются на сервис, который при помощи эвристического анализа отсекает подозрительный трафик и не пропускает его дальше. Борьба с DDOS-атаками собственными силами является творческой работой и требует от системного администратора или сетевого инженера большого опыта в настройке сетевых экранов и стрессоустойчивости, поскольку атаку придется отражать в реальном времени.

4. Сканирование локальной сети. Данный тип атак может быть совершен как злоумышленником извне, так и инсайдером. В результате сканирования выясняется топология локальной сети, доступные информационные ресурсы и сервисы. Информация, полученная в результате сканирования может использоваться для последующей атаки. Защита от сетевых сканеров подразумевает применение политики сетевых экранов. Поведенческие признаки программы-сканера легко выявить путем эвристического анализа.

5. Сканирование узлов локальной сети на предмет уязвимостей. Осуществляет поиск уязвимостей локальной сети, которые позже могут быть использованы для атаки. Достаточно сложный тип атаки для осуществления из-за пределов локальной сети.Защититься от сетевых сканеров можно при разработке и своевременном применении антивирусной политики и политики сетевых экранов.

6. Взлом или компрометация реквизитов доступа легального пользователя. Подобные атаки могут осуществляться как с помощью специального ПО, так и вручную:

- подбор пароля по словарю;

- получение пароля из свободного доступа (например, из стикера, наклеенного на монитор);
- получение пароля от пользователя при помощи методов социальной инженерии;
- получение пароля при помощи метода фиксации нажатия клавиш (при использовании вредоносного программного обеспечения).

7. Анализ сетевых протоколов. С помощью этого вида атаки, осуществляемого внутри локальной сети предприятия, можно перехватывать незашифрованную информацию. Классическим примером может служить веб-протокол HTTP, не имеющий шифрования. Учетные данные, передаваемые по данному протоколу, могут быть скомпрометированы. Решением проблемы подобных атак является разработка и применение политики безопасности информационных ресурсов компании и политики работы в сети Интернет.

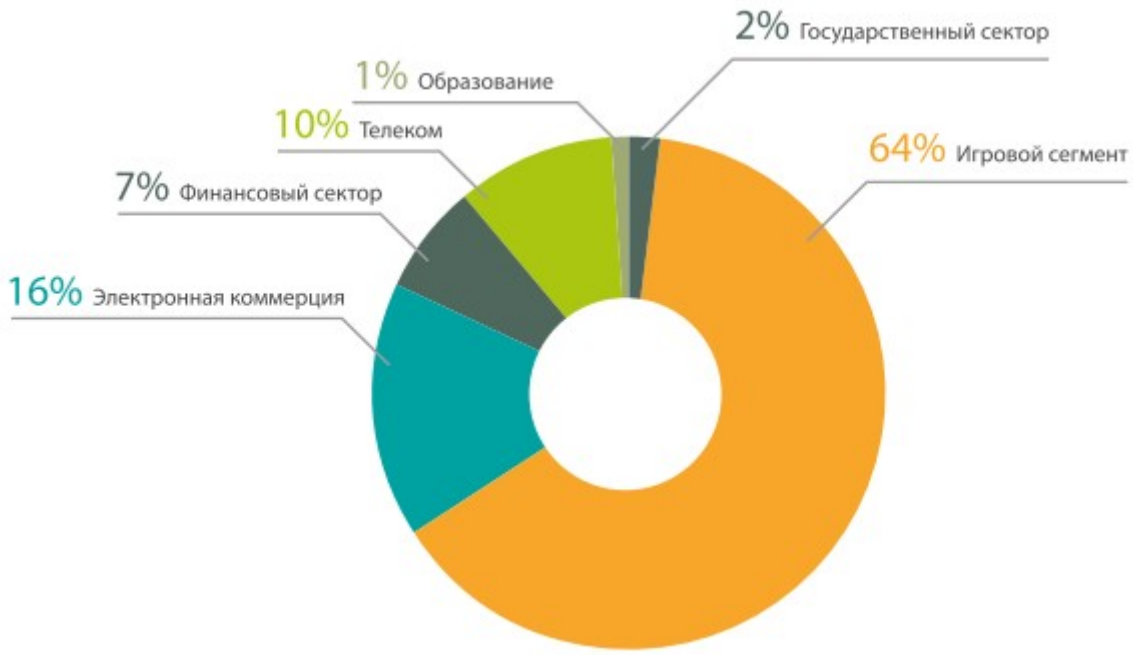

Рис. 1.3 – Статистика DDOS-атак по отраслям за 2019 год

Как правило, злоумышленники, осуществляющие атаки через сеть, для защиты от последующего обнаружения при расследовании инцидентов пользуются цепочкой промежуточных перенаправляющих серверов (прокси) или сетью Tor. Поэтому осуществление определение точного местоположения злоумышленника по IP-адресу не представляется возможным. Однако при использовании ботнетов для DDOS-атак адреса атакующих компьютеров могут соответствовать реальным. Диаграмма, представленная на рисунке 1.4 демонстрирует распределение кибератак по странам-источникам за 2019 год [36]. Можно заметить, что большая часть атак происходит с компьютеров или посредством прокси-серверов из СШАи Нидерландов. Это объясняется наличием огромного числа электронных устройств, использующих интернет в США и либеральным законодательством Нидерландов.

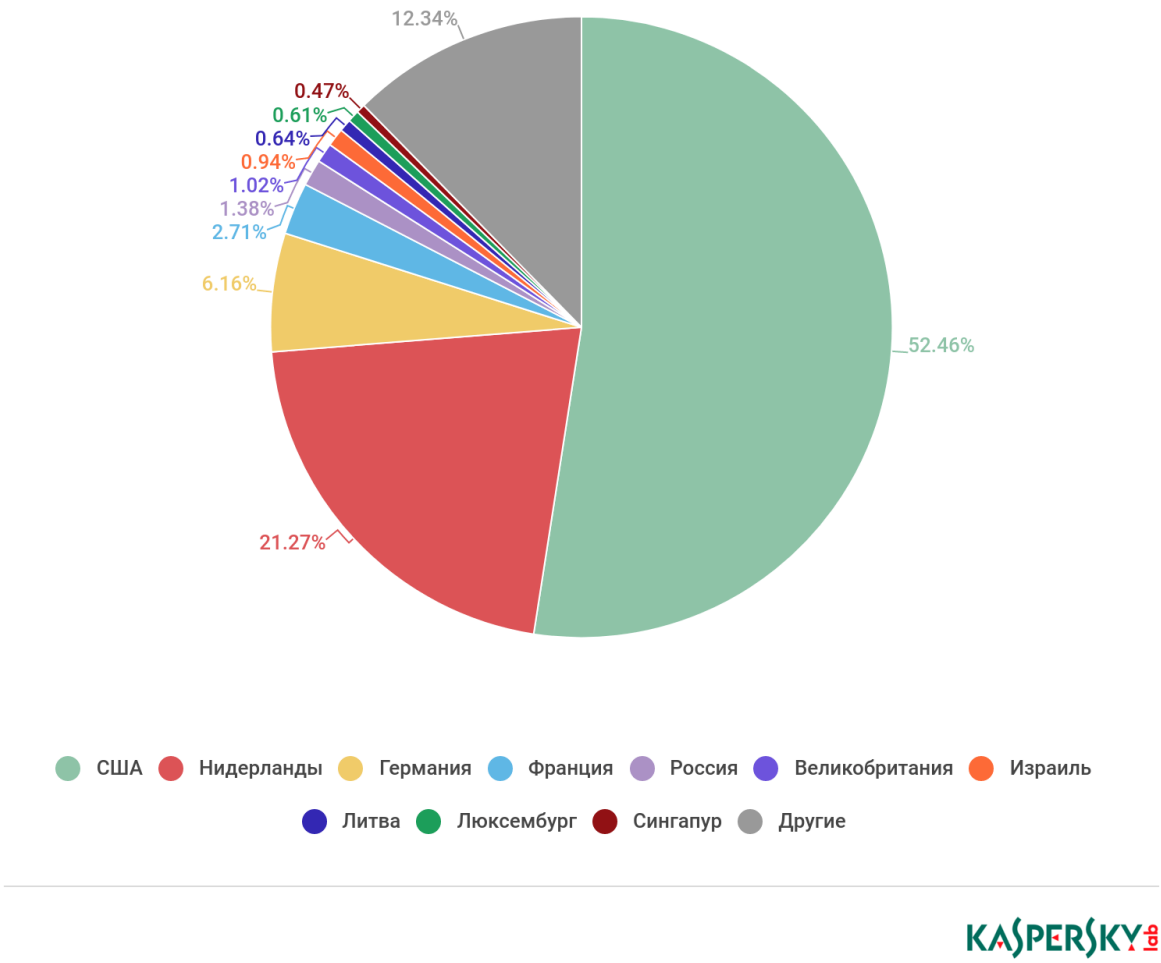

Рис. 1.4 – Распределение кибератак по странам-источникам за 2019 год

Задача правильно работающей системы информационной безопасности – не только отразить атаку, но и собрать максимум сведений для их последующей передачи в правоохранительные органы.

1.3 Современные подходы к анализу существующих систем информационной безопасности предприятий

Обследование информационных систем предприятия на предмет защищенности позволяет определить, работают ли

существующие механизмы безопасности информации, отвечают ли они существующим рискам, существуют ли потенциально опасные уязвимости.

Для того, чтобы получить ответ на эти вопросы, необходимо построить модель системы защиты с полным перекрытием. В данной модели взаимодействуют три сущности [23]:

- область угроз;
- защищаемая область;
- система защиты.

Отсюда вытекают три множества:

- $T = \{t_i\}$ – множество угроз безопасности;
- $O = \{o_j\}$ – множество ресурсов защищаемой системы;
- $M = \{m_k\}$ – множество механизмов защищаемой системы.

Отношения элементов вышеописанных множеств описывают систему защиты. Для описания используется графовая модель. Множество отношений «объект-угроза» образует двудольный граф [25]. Цель защиты объектов заключается в том, чтобы перекрыть все существующие ребра графа. Именно за это и отвечает множество M. С его введением граф становится трехдольным.

В процессе развития модели системы защиты с полным перекрытием вводятся еще два элемента:

1. V – множество уязвимых точек системы, определяемый как подмножество декартова произведения: $T * O$: $v_r = t_i * o_j$. Таким образом, уязвимость системы защиты есть ни что иное как возможность осуществления угрозы t в отношении объекта o.

2. B – множество барьеров, которое выражается декартовым произведением V * M: $b_i = t_i * o_j * m_k$. Эти барьеры определяют способы реализации угроз безопасности, перекрытые средствами защиты.

Таким образом, конечный вариант модели представляет собой пятиэлементную систему защиты с учетом имеющихся уязвимостей.

Модель системы с полным перекрытием предполагает, что для каждой уязвимости есть барьер, который её устраняет. Данное условие является одним из факторов, определяющих защищенность информационной системы. Вторым фактором является прочность механизмов защиты.

При идеальном построении системы защиты каждый механизм должен полностью исключать один из путей реализации угрозы. В реальных системах механизмы защиты обеспечивают ли некоторый уровень сопротивляемости угрозам. Для оценки набора барьеров B можно использовать набор $P_i * L_i * R_i$, где P_i – вероятность появления угрозы, L_i– степень серьезности угрозы (определяется как величина ущерба в случае реализации угрозы), R_i – степень сопротивляемости механизма защиты, которая характеризуется вероятностью его преодоления.

Прочность барьера оценивается при помощи величины остаточного риска $Risk_i$возможности реализациию угрозы t_iв отношении объекта информационной системы o_jпри использовании механизма защиты m_k (формула (2)).

$$Risk_i = P_k - L_k(1 - R_k) \quad (2)$$

Величину защищенности S можно оценить при помощи формулы (3).

$$S = 1 / \sum_{(\forall b_k \epsilon B)} (P ¿ ¿ k - L_k (1 - R_k)), \text{где } P_k, L_k \epsilon (0,1), R_k \epsilon ¿ (3) ¿$$

Знаменатель формулы (3) определяет сумму остаточных рисков как возможность реализации угроз T на объектах информационной системы O в случае использованиязащитных механизмов M. Показатель суммарной величины остаточных рисков является оценкой общей уязвимости системы защиты. Общая защищенность системы в данном случае будет обратно пропорциональна. Если в системе отсутствует система барьеров b_kсопротивляемость механизма защиты R_kприравнивается к нулю.

В реальности достигнуть точности при расчете характеристик барьеров достаточно сложно, так как понятия «угроза», «ущерб», «сопротивляемость механизма защиты» практически не поддаются формализации. Если защищаемая информация носит политический или военный характер, то величину ущерба в результате осуществления угрозы можно определить лишь с достаточно небольшой точностью, а для определения вероятности реализации угрозы уже недостаточно статистических выкладок.

Однако для экономической информации были разработаны стоимостные методы анализа эффективности средств защиты. Для их использования необходимо дополнить характеристики барьера при помощи величины C_i, которая представляет собой затраты на построение барьера b_i. При этом основной задачей оптимизации набора средств защиты является оптимизация суммарных затрат $W_i = \{w_i\}$, состоящих из затрат на создание барьеров C = $\{c_i\}$ и

потенциальных затрат в случае реализации угроз $N_i = \{n_i\}$.

Поскольку, как уже писалось выше, формализация элементов модели системы защиты с полным перекрытием вызывает большие трудности, распространение на практике получили подходы, основанные на неформальной классификации. Вместо формальных и стоимостных оценок в данных подходах используется категорирование. Выделяют следующие категории [29]:

1. Нарушители. Нарушителей можно классифицировать по целям, квалификации, доступным ресурсам.

2. Информация. Информацию можно условно разделить по степени конфиденциальности и критичности.

3. Средства защиты информации. Как правило, средства защиты информации классифицируются по надежности и функциональности.

Хотя категорирование не дает высокой точности показателей защиты, но позволяет присваивать информационным системам классы защищенности и сравнивать их между собой. На подобном принципе основан международный стандарт ISO 15408 «Общие критерии оценки безопасности информационных технологий» и национальный стандарт Российской Федерации ГОСТ Р ИСО/ МЭК 15408-1-2008 «Методы и средства обеспечения безопасности. критерии оценки безопасности информационных технологий».

1.4 Этапы процесса модернизации системы информационной безопасности предприятия

Задача модернизации системы информационной безопасности напрямую связано с понятием архитектуры системы информационной безопасности. Грамотное планирование архитектуры новой системы информационной безопасности в сочетании с соблюдением баланса между степенью защиты и стоимостью системы информационной безопасности обеспечивает ряд несомненных преимуществ. Правильное построение взаимосвязи между подсистемами позволяет снизить совокупную стоимость владения системой защиты информации, увеличить коэффициент возврата инвестиций, повысить управляемость системы и улучшить отслеживаемость событий информационной безопасности.

На рисунке 1.5 представлен цикл работ, которые нужно провести для модернизации системы информационной безопасности [35]. Он состоит из четырех больших блоков:

- обследование;
- проектирование;
- внедрение;
- сопровождение и обслуживание.

Обследование – важнейший этап процесса модернизации системы информационной безопасности. Чтобы выстроенная система была эффективна, процесс модернизации необходимо начинать с анализа угроз и уязвимостей информационной системы с последующим анализом рисков информационной безопасности. Обследование должно быть комплексным и охватывать все основные бизнес-процессы, информационную систему предприятия и существующие средства защиты информации. Аудит действующей системы информационной безопасности позволит понять,

соответствует ли безопасность информационных ресурсов организации необходимым требованиям и обеспечиваются ли целостность, доступность и конфиденциальность информации. После первичного обследования вся полученная информация формализуется и составляется описание существующих информационных ресурсов, сервисов и бизнес-процессов. Затем выполняется анализ угроз и уязвимостей. На этом этапе желательно также провести тесты на проникновение

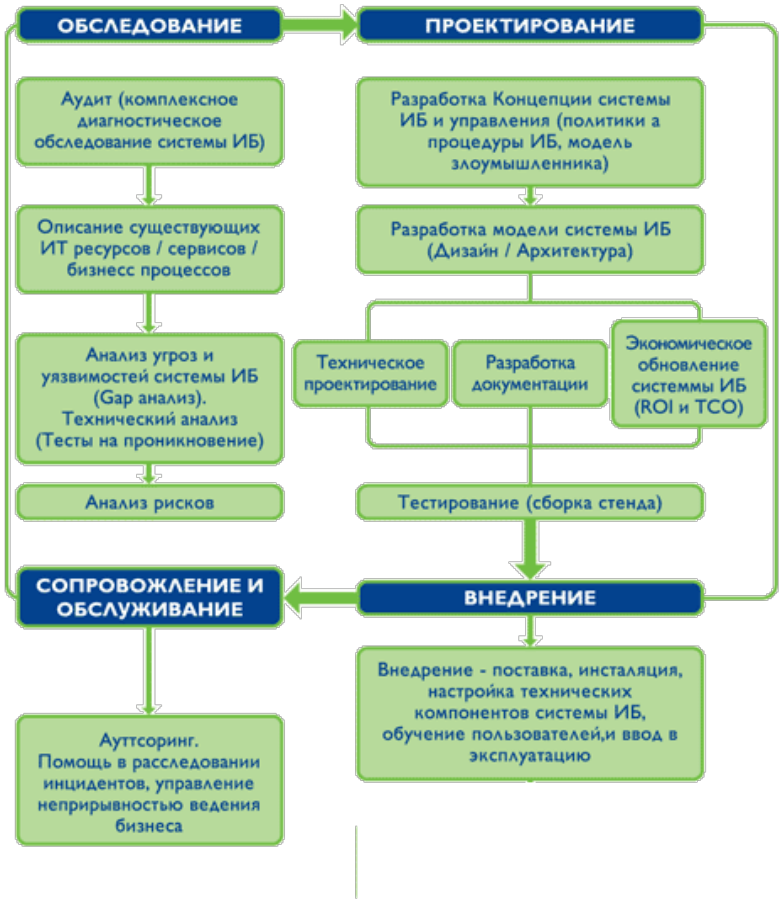

Рис. 1.5 – Полный цикл работ по обеспечению информационной безопасности

.

В процессе аудита системы выполняется следующее:

- определяются владельцы информационных ресурсов и ответственные за их целостность, формализуются требования к системе контроля прав доступа;
- все информационные ресурсы категоризируются по степени критичности для бизнеса;
- производится проверка всех процедур информационной безопасности: поддержка системы, методы расследования инцидентов в области информационной безопасности, организация системы резервного копирования, разделение прав пользователей, организация удаленного доступа к системе;
- определяются лица, ответственные за развитие и поддержку системы информационной безопасности.

Если аудит проводится силами компании-подрядчика, то необходимо на всех стадиях процесса привлекать сотрудников предприятия-заказчика. Это позволит учесть пожелания, требования и специфику обследуемой организации. При этом главным преимуществом использования аутсорсинга является возможность использовать накопленный опыт специалистов сторонней компании при анализе различных частей системы информационной безопасности на предмет соответствия требованиям защиты информации для определенной индустрии [22].

Проектирование системы информационной безопасности как задача напрямую связана с понятием «архитектура системы информационной безопасности». Современный подход к архитектуре систем информационной безопасности рекомендует использование интегрированной архитектуры.

Она подразумевает функционирование всех компонентов как единого комплекса с централизованным управлением.

Интегрированная архитектура системы информационной безопасности подразумевает в своем составе следующие подсистемы:

- подсистему защиты периметра сети и межсетевых взаимодействий (межсетевые экраны и т.п.);
- подсистему защиты серверов сети;
- средства защиты рабочих станций;
- подсистему мониторинга и аудита безопасности;
- средства обнаружения атак и автоматического реагирования;
- подсистему комплексной антивирусной защиты;
- средства анализа защищенности и управления политикой безопасности;
- средства контроля целостности данных;
- средства криптографической защиты информации;
- инфраструктуру открытых ключей;
- подсистему резервного копирования и восстановления данных;
- автоматизированную систему установки обновлений программного обеспечения;
- средства управления безопасности;
- подсистему аутентификации и идентификации.

Как уже было указано выше, архитектура системы информационной безопасности предполагает наличие системы управления информационной безопасностью. Перед системой управления стоят задачи систематизации процессов обеспечения информационной безопасности, расстановка приоритетов компании в этой области,

достижение адекватности и прозрачности системы, обеспечение механизма отслеживания вносимых в систему изменений и эффективности управления системой в критических ситуациях.

Процесс управления безопасностью отвечает за планирование, исполнение, контроль и техническое обслуживание всей инфраструктуры безопасности. Его организация значительно усложнена тем, что у компании есть бизнес-процессы, не связанные с информационными технологиями, но нуждающиеся в обеспечении информационной безопасности.

Проектирование системы информационной безопасности обычно состоит из следующих этапов [17]:

1. Разработка Концепции обеспечения информационной безопасности. Определяются основные цели, задачи и требования, а также общая стратегия построения системы ИБ. Идентифицируются критичные информационные ресурсы. Вырабатываются требования к системе ИБ и определяются базовые подходы к их реализации.
2. Создание / развитие политики ИБ.
3. Построение модели системы управления ИБ (на основе процессно-ролевой модели).
4. Подготовка технического задания на создание системы информационной безопасности.
5. Создание модели системы ИБ.
6. Разработка технически-рабочего проекта (ТРП) создания системы ИБ и архитектуры системы ИБ. ТРП по созданию системы ИБ включает следующие документы [29].

- пояснительную записку, содержащую описание основных технических решений по созданию системы ИБ и организационных мероприятий по подготовке системы ИБ к эксплуатации;

- обоснование выбранных компонентов системы ИБ и определение мест их размещения и описание разработанных профилей защиты;

- спецификацию на комплекс аппаратных средств системы ИБ;

- спецификацию на комплекс программных средств системы ИБ;

- определение настроек и режима функционирования компонентов системы ИБ.

7. Тестирование на стенде спроектированной системы ИБ.

8. Разработка организационно-распорядительных документов системы управления ИБ (политик по обеспечению информационной безопасности, процедур, регламентов и др.).

9. Разработка рабочего проекта (включая документацию на используемые средства защиты и порядок администрирования, план ввода системы ИБ в эксплуатацию и др.), планирование обучения пользователей и обслуживающего персонала информационной системы.

Как только спроектированная система информационной безопасности успешно спроектирована, можно перейти к следующему этапу – внедрению. Этот этап обычно включает в себя следующие работы:

- поставку необходимого аппаратного и программного обеспечения;

- установку программного обеспечения;
- настройку всех взаимодействующих подсистем и компонентов;
- проведение процедуры сдачи-приемки системы;
- установка и настройка системы управления информационной безопасностью;
- обучение пользователей;
- ввод системы в «боевую» эксплуатацию.

Для того, чтобы внедренная система в промышленной эксплуатации работала в соответствии с проектными задачами и характеристиками, необходимо обеспечить её поддержку и сопровождение. Сопровождение системы может осуществляться как силами сотрудников компании, так и при помощи сторонней организации. Если аудит, проектирование и внедрение системы информационной безопасности было отдано на аутсорс, разумным решением будет прибегнуть к услугам компании-подрядчика и в вопросе поддержки.

Если для организации процесса модернизации системы информационной безопасности предприятия было принято решение обратиться к компании-подрядчику, следует руководствоваться следующими критериями:

- хорошая репутация на рынке;
- опыт работы в сфере информационной безопасности;
- хорошая техническая оснащенность;
- желательно наличие статусов партнера у поставщиков программного и аппаратного обеспечения;
- предоставление круглосуточной поддержки.

При условии соблюдении этих критериев и своевременном контроле ответственным сотрудников

обследуемой компании процесс модернизации вполнеможно доверить стороннему подрядчику.

Выводы по разделу:

В данном разделе произведена постановка задач исследования и рассмотрены теоретические основы, изучена основная литература по рассматриваемой теме исследования. Отдельное внимание уделено основным угрозам информационной безопасности на малых, средних и крупных предприятиях. Рассмотрены современные подходы к анализу существующих систем информационной безопасности предприятий, а также основные этапы процесса их модернизации.

2 ХАРАКТЕРИСТИКА ПРЕДПРИЯТИЯ

2.1 Описание предприятия

Производственная практика была пройдена на предприятии ООО «Каскад», находящемся по адресу г. Пятигорск, ул. Московская, 68А. Предприятие осуществляет деятельность в области организации информационной безопасности. Предприятие оказывает следующие услуги:

- аттестация автоматизированных систем на предмет защиты конфиденциальной информации;
- аттестация защищаемых помещений на предмет защиты конфиденциальной информации;
- аттестация автоматизированных систем на предмет защиты государственной тайны;
- аттестация выделенных помещений на предмет защиты государственной тайны;
- аттестация средств изготовления и размножения информации на предмет защиты государственной тайны;
- специальные исследования технических средств на предмет защиты государственной тайны;
- специальные проверки технических средств на предмет защиты государственной тайны;
- аттестация информационных систем, работающих с персональными данными на предмет защиты конфиденциальных данных;
- аттестация государственных информационных систем на предмет защиты конфиденциальной информации;
- услуги по защите государственной тайны в сторонних организациях.

Организация также имеет филиалы в городах Краснодар и Севастополь.

2.2 Построение модели угроз информационной безопасности предприятий

При построении модели угроз информационной безопасности предприятия рекомендуется использовать национальный стандарт Российской Федерации ГОСТ Р 51275-2006 [2], методические документы ФСТЭК и стандарты Банка России. Процесс построения модели делится на следующие подпроцессы:

- поиск источников угроз информационной безопасности;
- выявление наиболее ценных активов;
- определение потенциально осуществимых угроз безопасности информационной системы предприятия и путей их осуществления.

В соответствии с документом ФСТЭК «Методика определения угроз безопасности информации в информационных системах», модель угроз информационной безопасности должна включать в себя следующие разделы:

- описание информационной системы;
- модель нарушителей;
- возможные угрозы безопасности.

Правильно построенные модели угроз в дальнейшем позволяют выстроить на свое основе план защиты от актуальных угроз, содержащий эффективные меры противодействия злоумышленникам.

Поскольку структура современных информационных систем предприятий неоднородна и сложна, для

формализации описания модели угроз разумно прибегать к объектно-ориентированному подходу. Зачастую модель угроз информационной безопасности требует рассмотрения ряда вопросов с нескольких сторон, поэтому для её описания можно использовать диаграммы языка UML, позволяющие представить структуру сложные объектов и процессов в различных ракурсах и необходимым уровнем детализации.

Для описания вариантов реализации угроз всем активам из всех потенциальных источников была использована диаграмма вариантов использования, представленная на рисунке 2.1.

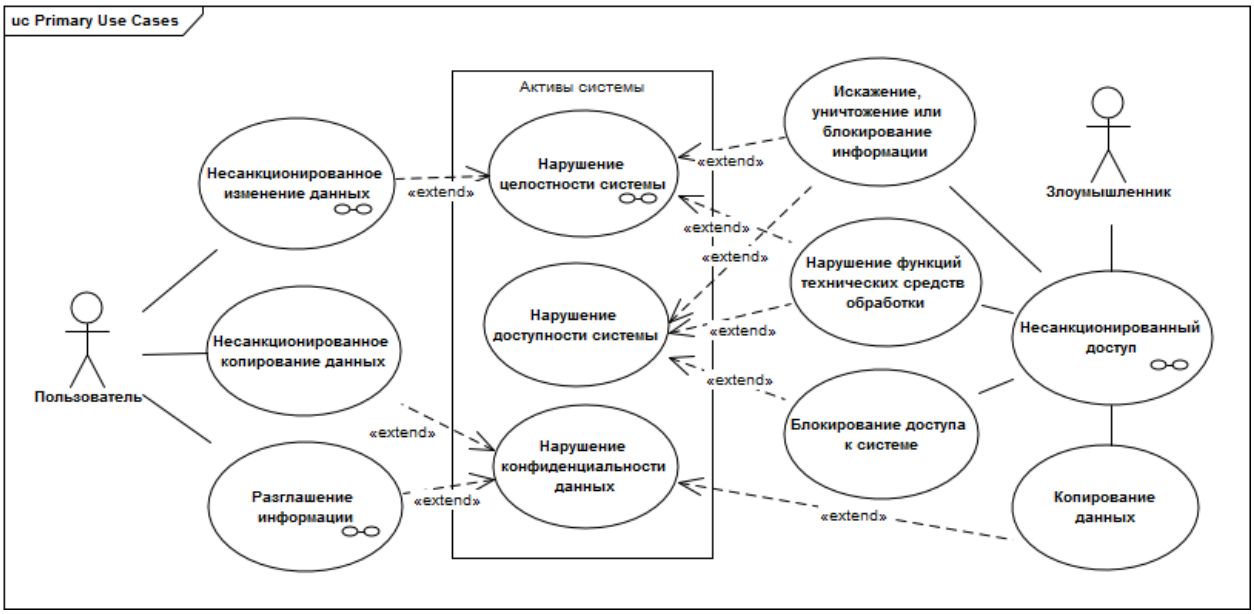

Рис. 2.1 – Концептуальная модель угроз информационной системы

На диаграммах данного типа используются обозначения в виде «человечков», называемые экторами (англ. Actor).Эктор– этомножество логически связанных ролей, исполняемых при взаимодействии с прецедентами или

сущностями (система, подсистема или класс). Эктором может быть человек или другая система, подсистема или класс, которые представляют нечто вне сущности.Обозначения в виде овалов называются прецедентами. Прецедент – это спецификация последовательности действий. Он описывает некоторый целостный фрагмент поведения системы, не вдаваясь при этом в особенности внутренней структуры субъекта.

Исходя из представленной выше диаграммы, способы реализации угроз – это тоже угрозы, расширяющие исходные угрозы. В данном случае язык UML позволяет прибегнуть к декомпозиции. На рисунках 2.2 и 2.3 приведены примеры декомпозиции угроз «несанкционированный доступ» и «разглашение информации».

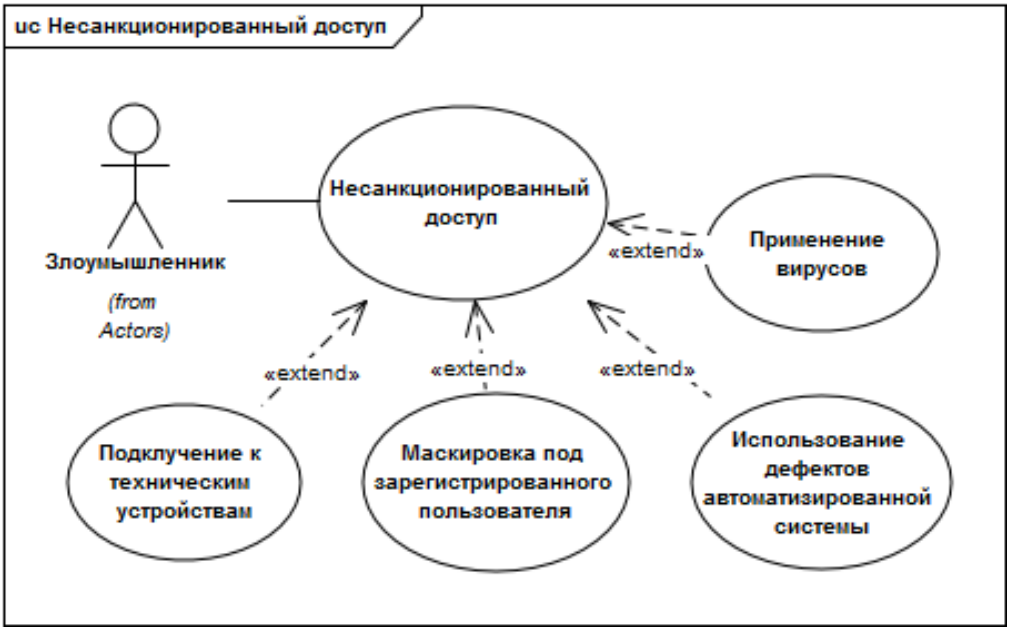

Рис. 2.2 – Способы реализации угрозы «Несанкционированный доступ»

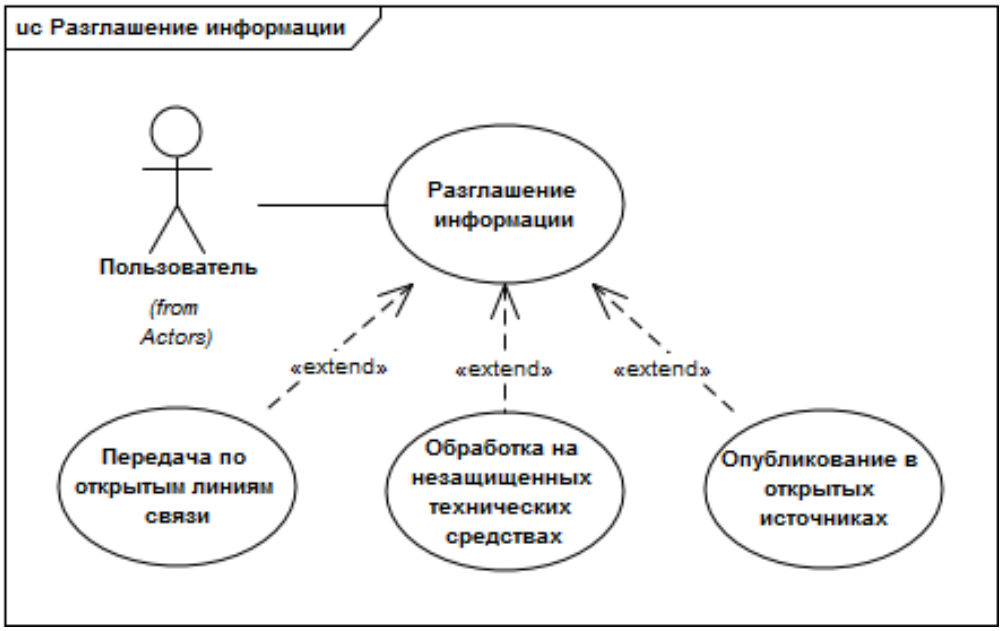

Рисунок 2.3 – Способы реализации угрозы «Разглашение информации»

Для анализа угроз в разрезе каждого отдельного актива можно использовать UML-диаграмму взаимодействия, которая демонстрирует связи между объектами моделируемой системы. На рисунке 2.4 рассмотрены угрозы активу «Целостность системы».

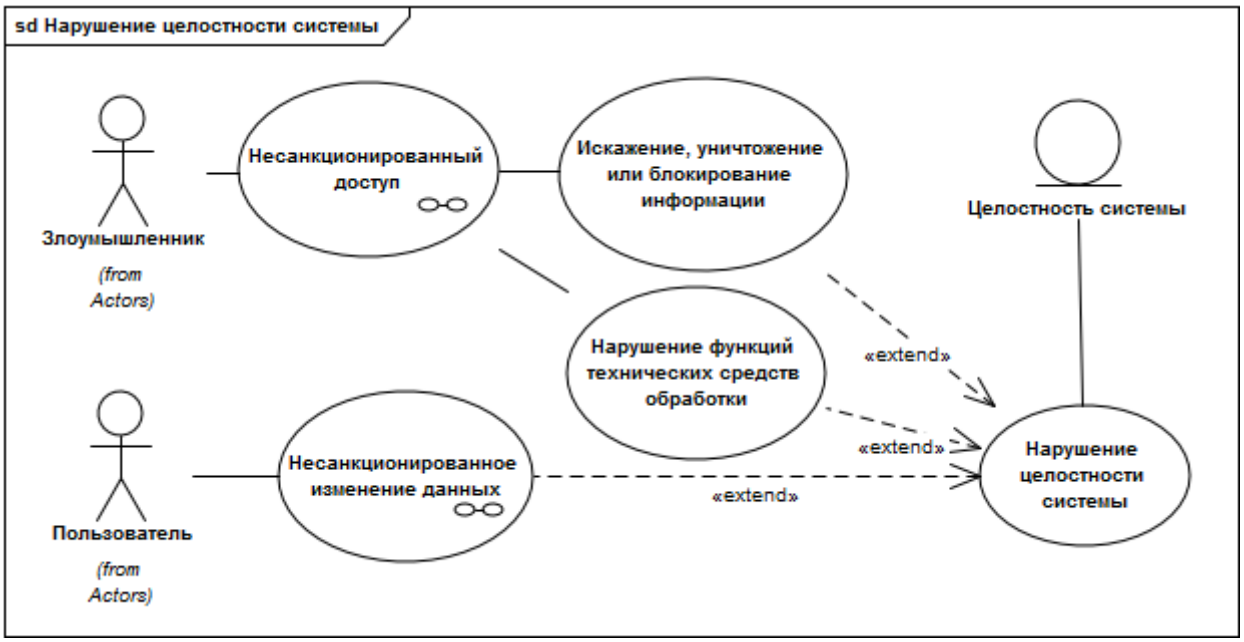

Рис. 2.4 – Угрозы активу «Целостность системы»

Для описания сценариев осуществления угроз можно воспользоваться диаграммами активности UML. Для каждой угрозы возможно построение двух сценариев:

- сценарий осуществления угрозы;
- сценарий защиты от угрозы.

Сценарий осуществления угрозы по своей сути представляет текущее состояние системы информационной безопасности. При моделировании такое состояние называется «AS IS», т.е «как есть». На рисунке 2.5 можно увидеть пример осуществления угрозы «Несанкционированное изменение данных».

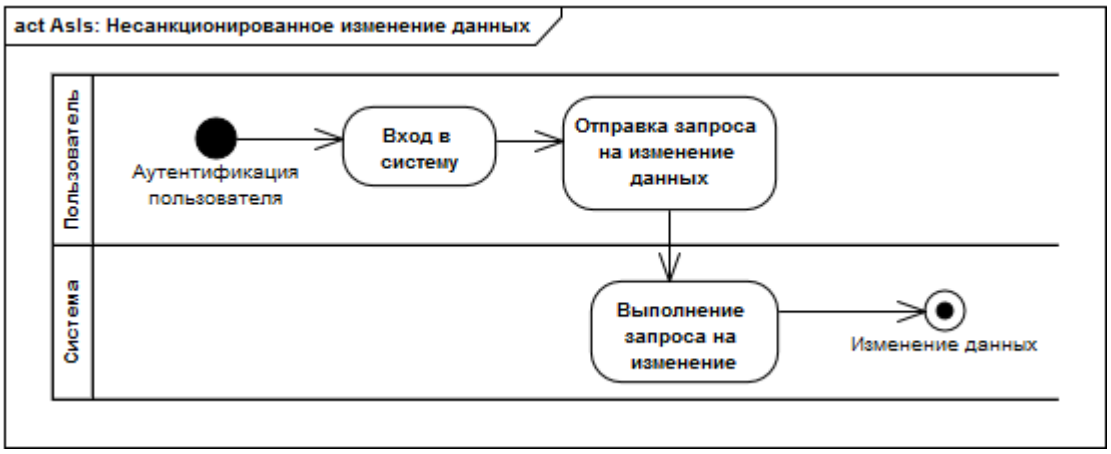

Рис.2.5 – Сценарий осуществления угрозы «Несанкционированное изменение данных»

Для моделирования модернизации системы информационной безопасности, иными словами, для

построения сценария противодействия угрозы выстраивается модель «TO BE» («как должно быть»). Пример сценария защиты от угрозы «Несанкционированное изменение данных» представлен на рисунке 2.6.

В представленной модели используются три контура защиты:

- проверка прав на выполнение операции, основанная на политике привилегий;
- проверка критичности изменений, использующая классификатор операций;
- логирование (регистрация в таблицах логов) операций.

Совокупно эти контуры защиты представляют из себя модуль защиты от угрозы «Несанкционированное изменение данных», предполагающий модернизацию существующей информационной системы. Подобная модель позволяет выстроить требования к информационной системе:

- применение политики разделяемого доступа к информации;
- разработка категорий критичности операций;
- реализация журналирования существующих операций;
- разработка программно-аппаратного комплекса подтверждения операций третьим лицом;
- разработка программно-аппаратного комплекса оповещения службы безопасности.

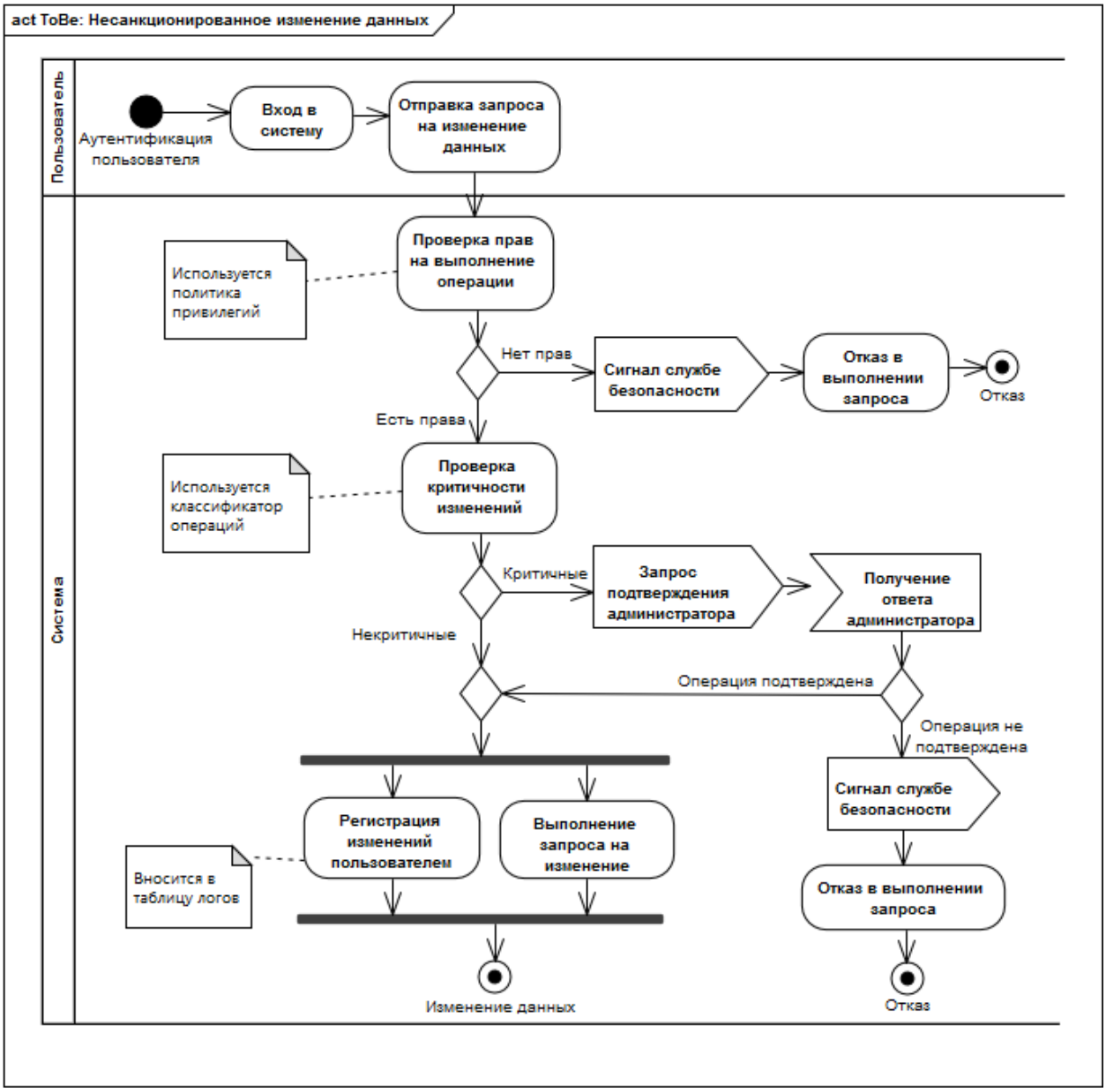

Рис 2.6 –Сценарий защиты от угрозы «Несанкционированное изменение данных»

На основании рассмотренных примеров можно построить модели угроз для информационных систем конкретных предприятий.

2.3 Типовые проблемы существующих систем информационной безопасности и методы их решения

Существующие систем информационной безопасности многих предприятий находятся не в самом лучшем состоянии. Статистика дает мало данных, поскольку для её формирования требуется проводить аудиты в каждой организации. Но, согласно, имеющимся данным, большая часть проблем информационной безопасности, с которыми сталкиваются современные предприятия, являются типовыми [31, 33]. Следует рассмотреть наиболее встречающиеся проблемы подробнее.

Как правило, на большинстве отечественных предприятий достаточно слабо проработана организационная составляющая. Информация не классифицирована по типам с точки зрения конфиденциальности и критичности для бизнеса. Отсюда возникают сложности в обосновании целесообразности мер по защите информации и применении правовых методов расследования возникающих инцидентов.

Для решения этой проблемы необходимо выработать систему классификации информации и модель доступа к ней. Разработанные документы должны быть утверждены генеральным директором и поддерживаться в актуальном состоянии.

Следующая проблема связана с необходимостью обеспечения непрерывности функционирования информационных систем и высокого уровня доступности сервисов. Многие современные компании сильно зависят от бесперебойной работы информационных систем, поддерживающих бизнес. Сбои в работе этих систем приводят к прямым и косвенным финансовым издержкам. Зачастую причинами таких сбоев и нарушением доступа к

информации являются злонамеренные атаки извне, от которых и должна защищать система информационной безопасности [28].

Действительно, необдуманные требования политики безопасности могут приводить к сбоям в программном обеспечении и временным замедлениям или остановкам в работе информационных ресурсов и систем. Именно поэтому разработанные политики безопасности (например, политики доступа) подразделение, отвечающие за безопасность, должно согласовывать с подразделением, занимающимся автоматизацией бизнес-процессов. Только взвешенные и продуманные компромиссы могут помочь избежать проблемных для компании ситуаций.

Также является проблемой отсутствие четкой стратегии развития информационных систем предприятия. Автоматизация бизнес-процессов происходит хаотично, зачастую используется политика «латания дыр». Новые сервисы и системы добавляются без какой-либо связи с существующими и без учета их взаимосвязи. Естественно на таких предприятиях сложно встретить логично построенную и надежную систему информационной безопасности. При этом степень надежности и оценку покрытия рисков, как правило, не определялись. Также редкое явление – оценка экономической целесообразности системы информационной безопасности.

Безусловно, основой для решения данной проблемы является выработка четкой стратегии развития информационной структуры компании в ближайшие 5 лет. Также необходимо построить карту уже имеющихся сервисов и систем, определить требуемую степень интеграции для

повышения управляемости и исключения повторного ввода данных. После этого можно проводить полноценный аудит системы информационной безопасности.

Руководители среднего и нижнего звена, а также большая часть персонала не осознает потребности в проведении работ по улучшению состояния информационной безопасности. Корневой причиной этой проблемы является тот простой факт, что стратегические задачи компании представляются прозрачными только для менеджеров высшего звена. Средняя и нижняя часть руководящей цепочки видят только введение новых ограничений для пользователей, понижающих эффективность труда, а также увеличение затрат как на проведение работ, так и на поддержку системы информационной безопасности.

Решением данной проблемы может быть проведение семинаров для повышения квалификации сотрудников в области информационной безопасности, а также информирование всех сотрудников о стратегических задачах компании.

Еще одна известная проблема – противостояние отдела, отвечающего за автоматизацию бизнес-процессов и отдела информационной безопасности. Сложность заключается в том, что ответственность за информационную безопасность несет один отдел, а её реализацией занимается другой. Отдел автоматизации часто не хочет решать дополнительные проблемы, вызванные ограничениями безопасности, поскольку, во-первых, это создает дополнительную работу, а во-вторых, может приводить к задержке или остановке бизнес-процессов, что несет компании финансовые и репутационные потери.

Для решения подобных разногласий необходимо организационно подчинить оба отдела одному начальнику и привести технологическую и организационную документацию в такой вид, который правильно разграничивал бы сферы ответственности обоих отделов.

Личная заинтересованность руководителей среднего или высшего звена в результатах работ по исследованию защищенности информационной системы предприятия тоже может оказаться проблемой. Данные, полученные в результате исследования, используются не в служебных целях, а для получения личной выгоды в том или ином виде. Результаты исследования могут толковаться именно так, как требует «политическая» ситуация внутри организации, что ведет к искажению смысла.

Подобная проблема должна выявляться на высшем уровне руководства и немедленно пресекаться. Быстрое и своевременное противодействие – единственный способ решения проблемы.

Проблемы часто возникают уже при попытке модернизации текущей системы информационной безопасности [24]. К примеру, аудит текущей системы производится независимой компанией. Она предоставляет отчет о текущих проблемах информационной безопасности и рекомендации по их устранению. Практическая реализация рекомендаций может выполняться своими силами. При этом препонами реализации проекта могут стать внутренняя бюрократия, нерасторопность отдельных сотрудников, их некомпетентность или недостаточная информированность.

Избежать подобных проблем можно, назначив руководителем проекта одного из менеджеров высшего

звена. В некоторых ситуациях исполнение проекта необходимо контролировать самому генеральному директору. Альтернативным вариантом решения может быть полная передача задачи модернизации существующей системы информационной безопасности на аутсорсинг. Тем не менее, курировать проект со стороны заказчика также должен представитель высшей части руководящего звена.

Также проблемой может стать низкая квалификация сотрудников, занимающихся информационной безопасностью, которая может не позволить им поддерживать созданную систему безопасности.

Проблема решается включением в план модернизации системы информационной безопасности обучения ответственных сотрудников с целью повышения их квалификации, а также организации общих обучающих семинаров для остальных сотрудников

При разработке плана модернизации существующей системы информационной безопасности на предприятии следует учитывать вышеописанные проблемы и заранее предусматривать в плане меры по их решению.

2.4 Разработка концепции информационной безопасности

Концепция информационной безопасности представляет собой методологический комплекс нормативных технических документов, предназначенных для решения следующих задач:

- разработки требований информационной безопасности по защите информационных систем предприятия от несанкционированного доступа;

- построения или модернизации защищенных информационных систем;

- сертификации информационных систем.

Концепция информационной безопасности – высокоуровневый документ. Он определяет стратегию развития информационной безопасности предприятия и дальнейшее масштабирования системы защиты. Для практической реализации на основании концепции информационной безопасности формируется политика информационной безопасности, а на её основе, в свою очередь – детальные политики, инструкции, регламент и другие документы более низкого уровня (см. схему на рисунке 3.1).

Рис. 3.1 – Структура нормативной документации по информационной безопасности

Концепция информационной безопасности должна определять:

- информационные ресурсы и сервисы, которые нуждаются в защите;
- основные принципы защиты информации;
- требования к безопасности;
- организационные и технические меры обеспечения безопасности;
- ответственность сотрудников за соблюдения требований информационной безопасности.

Рекомендуется включать в структуру концепции информационной безопасности следующие разделы:

1. Общие положения.
2. Описание объекта защиты.
3. Основные факторы, влияющие на информационную безопасность предприятия.
4. Основные принципы обеспечения информационной безопасности.
5. Организация работ по защите информации.
6. Меры обеспечения информационной безопасности.
7. Распределение ответственности и порядок взаимодействия.
8. Порядок категорирования защищаемой информации.
9. Модель нарушителя информационной безопасности.
10. Модуль угроз информационной безопасности.
11. Требования к обеспечению информационной безопасности.
12. Технические требования к смежным подсистемам.
13. Ответственность сотрудников за нарушение безопасности.
14. Механизм реализации концепции.

Нормативная база, на которой будет основываться концепция безопасности может быть выбрана в зависимости от географического рынка, на который ориентируется компания. Если компания является международной, ей стоит руководствоваться международными стандартами SO/IEC 27001-2005, ISO/IEC 17799-2005, ISO/IEC TR 13335. В случае, если компания российская, ей требуется обеспечивать корректную обработку персональных данных. В данном случае лучше опираться на национальный стандарт ГОСТ Р ИСО/МЭК 15408 [1].

Правильно выстроенная концепция информационной безопасности значительно снижает ресурсы на формирование нижестоящих политик безопасности.

2.5 Разработка политики информационной безопасности

Политика информационной безопасности представляет собой совокупность организационно распорядительных и нормативно-методических документов. В более узком понятии политика безопасности является единый документ, определяющий общие принципыбезопасности внутри организации. Документ должен быть понятен всем сотрудниками организации, все специализированные термины должны быть перенесены в подчиненные документы, на которые будет ссылаться политика безопасности. Рекомендуется соблюдать максимально возможную лаконичность и простоту изложения, поскольку именно с этим документом должен будет ознакомиться каждый сотрудник организации. Регламенты, графические

схемы, детальные политики должны быть вынесены в приложения. Наиболее оптимальной является четырехуровневая схема документа [27]:

1. Непосредственно сама политика информационной безопасности.
2. Положение об информации, составляющей коммерческую тайну.
3. Положение об информации, являющейся персональными данными.
4. Регламенты, методики, детальные политики.

Следует помнить о том, что политика информационной безопасности, не может быть универсальна. Уникальная комбинация таких факторов, как территориальное подразделение, специфика отрасли, графики работы, доступные ресурсы, количество сотрудников, среднегодовой доход при разработке политики требует учета каждого из них.В зависимости от набора угроз разработчик политики информационной безопасности обязан определить специфику защитных мер. Эти меры, с одной стороны, должны обеспечивать максимально возможную степень безопасности, а с другой – разумно подходить как к общей стоимости выстраиваемой системы, так и к затратам на поддержку дальнейшей эксплуатации. К тому же, необходимо соблюсти самое сложное условие: разрабатываемые в рамках политики безопасности регламенты не должны негативно влиять на производительность труда.

Если политика информационной безопасности разрабатывается в крупной организации, необходимо учесть фактор бюджетирования. Внедрение или модернизация политики информационной безопасности неизбежно

потребует косвенных или прямых финансовых затрат. Необходимо предоставить эти сведения в финансовые и бухгалтерские службы организации для своевременной корректировки бюджета. При этом необходимо учитывать график затрат, поскольку изменения могут занять до полугода.

Таким образом, в процессе разработки политики необходимо взаимодействие разработчика политики с финансовыми подразделениями предприятия и руководством. Это справедливо как при разработке своими силами, так и с применением услуг сторонних организаций.

Выводы по разделу:

В данном разделе приведены краткие сведения о предприятии, на котором была пройдена производственная преддипломная практика, рассмотрены принципы построения модели угроз информационной безопасности предприятий, а также типовые проблемы существующих систем информационной безопасности. Проанализированы подходы к построению концепции и политики информационной безопасности.

3 ПРОЕКТНАЯ ЧАСТЬ

3.1 Разработка плана модернизации системы информационной безопасности

При разработке плана модернизации системы информационной безопасности необходимо учитывать целый ряд факторов [23]:

1. Требуемый класс защищенности системы.
2. Отраслевые особенности.
3. Централизацию или децентрализацию управления.
4. Особенности географического положения.
5. Средний годовой доход.
6. Количество и физическое местоположение информационных ресурсов.
7. Количество сотрудников.

План модернизации основывается на уже разработанных концепции и политике информационной безопасности, в которых учтены особенности конкретной организации в отношении защищаемых активов, ответственных лиц, управляющего совета и комитета по внедрению. Однако, разработанные документы не учитывают, к примеру, особенностей бюджетирования в организации, текущей квалификации штатных специалистов по информационной безопасности и рядовых сотрудников компании, микроклимата в коллективе и нюансов взаимоотношения между отделами, и многого другого.

Типичная ошибка при формировании плана внедрение – расчет сроков отдельных работ по реально затраченному на них времени. Любая модернизация системы информационной

безопасности на предприятиях, где работают люди, во-первых, требует тесного взаимодействия с ними, а во-вторых, никогда не укладывается в планируемые сроки. Поэтому необходимо весьма осторожно подходить к оценке временных затрат, особенно, если работы по модернизации системы информационной безопасности проводятся сторонней организацией.

План модернизации должен предусматривать защиту от потенциального сопротивления внедрению (вплоть до саботажа) как отдельных сотрудников, так и целых подразделений.

Отдельное внимание в плане модернизации следует уделить повышению квалификации штатных специалистов по информационной безопасности, а также улучшению общих познаний сотрудников.Допустимо проводить обучение поэтапно:

1. Повышение квалификации в области информационной безопасности у руководства.
2. Повышение квалификации в области информационной безопасности у ответственных специалистов.
3. Повышение квалификации в области информационной безопасности у остальных сотрудников силами ответственных специалистов.

План внедрения должен утверждаться специальным комитетом, состоящим из сотрудников организации. В комитет должны входить руководители высшего звена компании, а также представители всех подразделений, участвующих в бизнес-процессах компании. В комитет также должен входить штатный специалист по информационной

безопасности, который назначается консультантом по общим вопросам. При возникновении ситуаций, в которых сотрудники сомневаются, будет ли соответствовать их решения регламентам и политике информационной безопасности, они могут обратиться к консультанту для разрешения противоречий.

Технико-экономическая часть плана внедрения должна включать перечень аппаратного и программного обеспечения, которое необходимо для реализации разработанной политики информационной безопасности с расчетом затрат на приобретение, пуско-наладочные работы и примерной стоимости эксплуатации. Необходимо также учитывать стоимость повышения квалификации системных администраторов для работы с новым оборудованием и программным обеспечением.

3.2 Необходимое аппаратное обеспечение системы защиты информации

Аппаратные средства обеспечения информационной безопасности можно разделить на несколько групп. Описание этих групп сведено в таблицу 3.1.

Таблица 3.1

Классификация аппаратных средств обеспечения информационной безопасности

№	Группа	Примеры устройств	Описание
1	Средства обеспечения сетевой безопасности	Мартшрутизаторы, коммуникаторы, сетевые экраны, устройства фильтрации трафика, комплексы защиты от	Обеспечивают защиту информационной системы предприятия от сетевых атак

		DDOS-атак	
2	Средства обеспечения контроля доступа в помещения	Контроллеры доступа в помещения, персональные идентификаторы, считыватели идентификаторов, турникеты, электронные замки	Обеспечивают защиту помещений предприятия от проникновения посторонних лиц
3	Средства оповещения о чрезвычайных ситуациях	Пожарная и охранная сигнализации (контроллеры, извещатели, оповещатели, источники резервного питания, пульты управления)	Обеспечивают защиту сотрудников, материальных ценностей и помещений предприятия от пожара и проникновения посторонних лиц с преступными намерениями
4	Средства видеонаблюдения	Видеорегистратор, видеокамеры	Обеспечивает визуальный контроль безопасности

Применение средств сетевой безопасности зависит от топологии локальной сети предприятия. Как правило, структурно сеть делится на три уровня [25]:

1. Уровень доступа. Он включает в себя коммутаторы для подключения конечных устройств: рабочих станций пользователей, сетевых принтеров и т. д. В современных реалиях пропускная способность сети на уровне доступа не должна быть меньше 1 Гбит/с (стандарт GigabitEthernet).

2. Уровень агрегации. Как правило устройства этого уровня предназначены для связи устройств уровня доступа между собой. Из этого следует, что устройств уровня агрегации может быть значительно меньше, чем устройств уровня доступа, однако они должны обладать большей вычислительной мощностью и высокой пропускной способностью. Рекомендуется пропускная способность не менее 10 Гбит/с.

3. Ядро сети. Устройства уровня ядра сети контролируют всю локальную сеть. Соответственно, к ним предъявляются большие требования, чем к устройствам уровня агрегации. На данном уровне пропускная способность сети может составлять 40 Гбит/с и выше.

Безусловно, речь идет о сети на средних и крупных предприятиях. Когда используется локальная сеть малых размеров, зачастую отказываются от уровня агрегации.

В случае, если предприятие является бюджетным или казенным учреждением, есть возможность подумать об импортозамещении, хотя в области сетевого оборудования могут возникнуть определенные проблемы с поставщиками. В таблице 3.2 представлены сравнительные характеристики российских производителей сетевого оборудования.

Если же не требуется ограничиваться российским производителем, рекомендуется использовать оборудования Cisco или Microtik/Huawei в качестве бюджетной альтернативы.

Таблица 3.2

Сравнение российских производителей сетевого оборудования

№	Наименование компании	Технологичность	Комплектность	Информационное обеспечение
1	Натекс	Отвечает современным требованиям	В наличии только коммутаторы уровня доступа	Курсы и учебные пособия в открытом доступе отсутствуют
2	Zelax	Отвечает современным	Не хватает коммутаторов уровня	Курсы и учебные пособия в открытом доступе отсутствуют

		требования м	агрегации	
3	Компания «Морион»	Оборудование морально устарело	Не хватает коммутаторов уровня ядра	Курсы и учебные пособия в открытом доступе отсутствуют
4	Elsicom	Отвечает современным требованиям	Не хватает коммутаторов уровня ядра	Курсы и учебные пособия в открытом доступе отсутствуют
5	Eltex	Отвечает современным требованиям	Не хватает коммутаторов уровня ядра	Курсы и учебные пособия в открытом доступе отсутствуют. Есть база знаний
6	Русьтелетех	Отвечает современным требованиям	Не хватает коммутаторов уровня ядра	Курсы и учебные пособия в открытом доступе отсутствуют. Существуют курсы в Нижегородском государственном техническом университете
7	Qtech	Отвечает современным требованиям	В наличии полная линейка оборудования	Курсы и учебные пособия в открытом доступе отсутствуют.

Сетевое оборудование должно обладать встроенными механизмами защиты от распространенных сетевых атак:

- переполнения CAM-таблицы коммутатора;
- MAC-спуфинга;
- ARP-спуфинга;
- подмены DHCP-сервера.

Каждое сетевое устройство должно быть управляемым и поддерживать технологию VLAN. При окончательном выборе оборудования следует также обратить внимание на пропускную способность и ряд других характеристик,

зависящих от размеров локальной сети, однако это выходит за рамки данной работы.

Система контроля и управления доступом (СКУД) является неотъемлемой частью комплексной системы охраны объекта, обеспечивает защиту имущества, недвижимости и сотрудников. Современные СКУД способны интегрироваться в общую систему безопасности объекта. Помимо безопасности внедрение СКУД дает следующие преимущества:

1. Бизнес-аналитика. На базе программно-аппаратного комплекса СКУД можно выстроить систему аналитики. Интеграция с системами кадрового и бухгалтерского учета, CRM, системами документооборота позволяют осуществлять автоматический обмен данными и их последующую обработку.

2. Сокращение затрат на охрану. Помимо прямых сокращений расходов на зарплаты охранников, современные СКУД позволяют сокращать расходы за счет автоматизации некоторых процессов.

3. Учет рабочего времени . СКУД позволяет учитывать вход и выход сотрудников с объекта, время посещений отдельных кабинетов.

СКУД состоит из следующих компонентов [14]:

1. Идентификаторы. Роль идентификатора может играть любой материальный предмет, являющийся носителем кодовой информации. Идентификатор может быть искусственно сгенерированным или уже существующим (например, биометрические данные). Наиболее часто используются следующие типы идентификаторы:

- бесконтактные радиоэлектронные (карты, брелоки, метки браслеты, смартфоны);
- биометрические (отпечатки пальцев, венозный рисунок руки, геометрия лица, радужная оболочка, рисунок сетчатки);
- контактные ключи;
- пин-коды.

2. Считыватели. Выбор считывателя, безусловно, зависит от типа выбранных идентификаторов. Типы считывателей совпадают с типами идентификаторов. Особое внимание следует уделить биометрическим считывателям. Они обладают следующими преимуществами:

- более высокий уровень защищенности по сравнению с традиционными системами идентификации;
- невозможность передачи идентификатора другому сотруднику или постороннему лицу;
- уменьшение вероятности мошенничества на проходных и рабочих местах;
- снижение рисков утраты идентификаторов и утечки персональных кодов;
- сокращение финансовых издержек на управление системой безопасности;
- отсутствие необходимости в запоминании паролей;
- высокая точность идентификации.

В соответствии с федеральным законом Российской Федерации «О защите персональных данных» биометрические признаки хранятся не в открытом виде, а в качестве некоторой цифровой последовательности. Принцип формирования последовательности похож на принцип формирования хэш-сумм, поэтому восстановить по

последовательности исходный биометрический признак невозможно.

3. Турникеты. Относятся к типу электромеханических преграждающих устройств. Турникеты обладают важной особенностью: они позволяют отсекать входящих по одному человеку. Существуют следующие типы турникетов:

- триподы (см. рисунок 3.1);
- с распашными створками (см. рисунок 3.2);
- с раздвижными створками (см. рисунок 3.3);
- полноростовые роторные (см. рисунок 3.4);
- полуростовые роторные (см. рисунок 3.5);
- шлюзовые (см. рисунок 3.6).

Рис. 3.1 – Турникет-трипод

Рис. 3.2 – Турникет с распашными створками

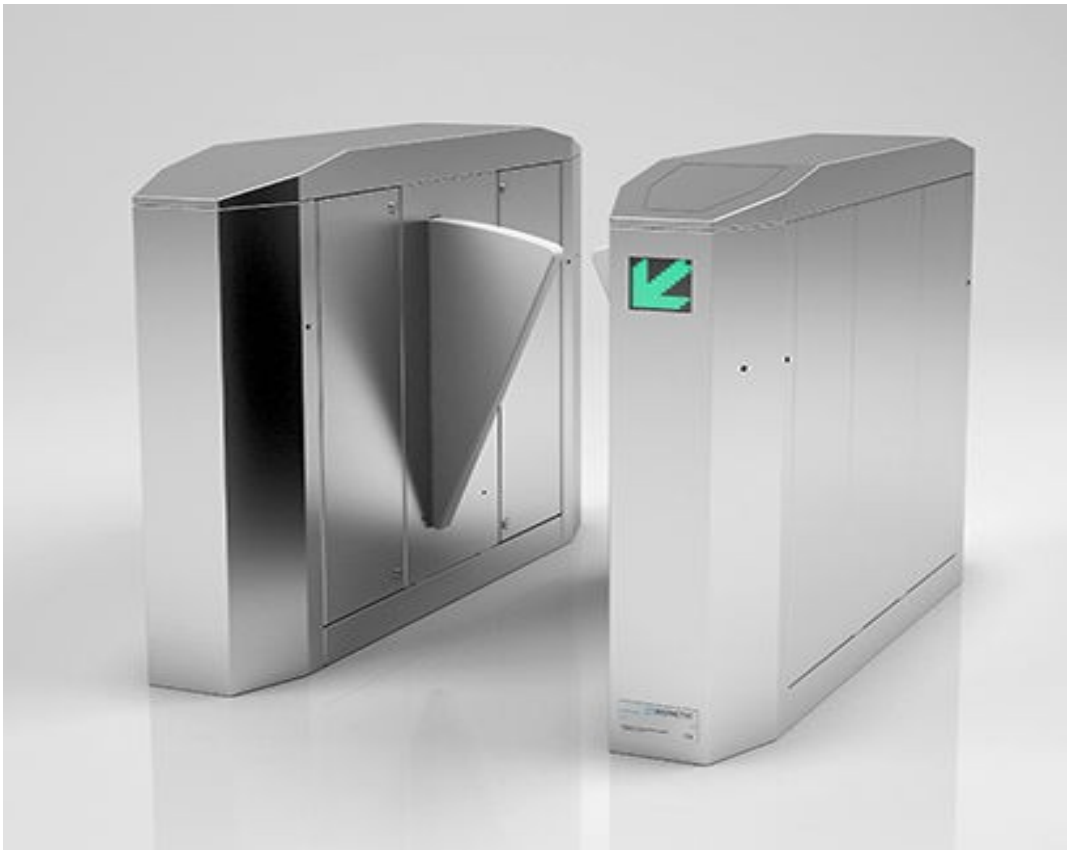

Рис. 3.3 – Турникет с раздвижными створками

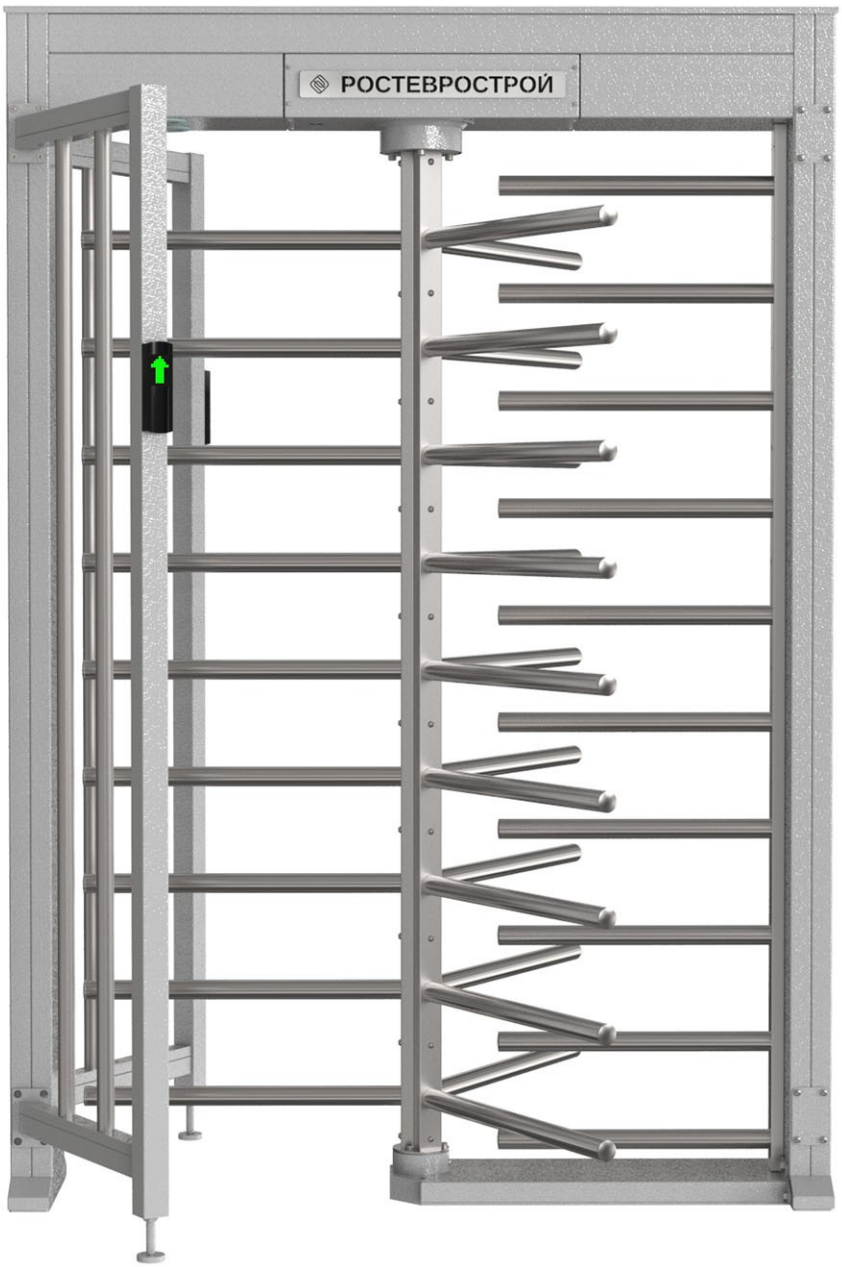

Рис. 3.4 – Полноростовой роторный турникет

Безусловно, выбор турникета должен основываться в соответствии с требуемым уровнем безопасности и исходя из экономической целесообразности. Все перечисленные типы турникетов за исключением полноростового роторного и шлюзового требуют физического контроля, поскольку

злоумышленник способен перелезть или перепрыгнуть через них.

Рис. 3.5 – Полуростовой роторный турникет

Рис. 3.6 – Шлюзовый турникет

Полноростовые турникеты, однако, требуют установки дополнительных заграждений соответствующего размера. Немаловажным фактором является ценовой: к примеру, стоимость полноростового роторного турникета более чем в 7 раз превышает стоимость трипода.

4. Электрозамки. Существуют следующие виды электрозамков:

- электромеханические замки;
- электромеханические защелки;
- электромагнитные замки;
- электроригельные замки.

Электромеханические замки могут устанавливаться как снаружи, так и внутри помещений. Как правило, внутри такие замки снабжаются кнопкой открытия. Открытие снаружи осуществляется за счет считывателя идентификаторов, подключенного к контроллеру СКУД.

Электромеханическая защелка представляет собой упрощенную версию электромеханического замка, а именно – его ответную часть, которая применяется совместно с обычным механическим замком. Защелки могут быть использованы как бюджетный вариант запорных механизмов, но крайне не рекомендуются для установки на режимных объектах и в помещениях с материальными ценностями.

Электромагнитный замок – еще один вид запирающего устройства, принцип работы которого заключается в следующем: в корпусе замка находится электромагнит, взаимодействующий с ответной планкой, которая изготовлена из сплава с высокой магнитной проницаемостью.

Данный тип замка требует постоянного электропитания и должен устанавливаться совместно с автономными источниками бесперебойного питания.

Электроригельный замок (также называется соленоидным) – компромисс между сложностью и надежностью замка. Запирание замка осуществляется за счет выдвижного ригеля, входящего в ответную часть.

5. Контроллеры СКУД. Контроллер является центральной частью управления СКУД. Он решает задачи управления остальными устройствами, хранение базы данных идентификаторов и журнала событий. Контроллеры могут быть как автономными, так и сетевыми.

Автономные контроллеры СКУД не способны работать в связке с другими контроллерами. Соответственно, централизованное управление такими контроллерами невозможно, поэтому настройку и управление базой данных пользователей необходимо производить непосредственно на самом контроллере. Именно по этой причине такие контроллеры не рекомендуются для использования в средних и крупных организациях.

Сетевые контроллеры СКУД могут объединены в одну сеть с централизованным управлением. С помощью специального программного обеспечения можно управлять доступами в помещения всего предприятия, а также интегрировать управление СКУД с системами жизнеобеспечения и управления предприятием.

Пожарная сигнализация – важная часть системы безопасности предприятия. Её основная задача – сберечь жизни и здоровье сотрудников, имущество организации. В качестве одной из второстепенных задач можно выделить

защиту информационной системы предприятия от фактора стихийного бедствия.

Пожарная сигнализация представляет собой сеть электронных устройств, построенных по топологии «звезда». Она состоит из следующих компонентов:

- приемно-контрольного прибора;
- пульта управления;
- извещателей;
- звуковых и световых оповещателей;
- исполнительных и релейных блоков;
- блоков резервного питания.

Пожарные извещатели выполняют задачу обнаружения пожара по его начальным признакам. Используются дымовые оптические извещатели для обнаружения дыма, извещатели пламени для обнаружения пламени, тепловые датчики для реакции на повышение температуры в помещении и ручные извещатели для поступления сигнала тревоги от человека. Существуют также комбинированные извещатели. Тип извещателя стоит выбирать в зависимости от специфики помещения. Стандартным набором является дымовой датчик и датчик открытого пламени, поскольку только такая комбинация дает близкую к 100% вероятность своевременного обнаружения пожара. Не стоит также пренебрегать и ручными извещателями.

Для оповещения о угрозе пожара служат оповещатели. Они могут быть световыми (таблички и информационные табло) и звуковыми.

Приемно-контрольный прибор получает сигналы со всех датчиков и управляет оповещателями. Приемно-контрольные

приборы можно классифицировать по следующим принципам:

- информационная емкость (количество шлейфов, которое способен обслуживать прибор);
- информативность (количество извещений, выдаваемых прибор)
- способ контроля извещателей (цифровой или аналоговый);
- тип каналов связи (проводные или радиоканалы).

Пульт управления служит для получения данных о том, где произошло возгорание. Следует отметить, что существует адресная и безадресная версия пожарных сигнализации. В безадресном исполнении на одном шлейфе могут находиться несколько датчиков из разных помещений. При срабатывании определенной зоны на пульте оператору приходится осмотреть все помещения, «закрепленные» за данной зоной. Адресная пожарная сигнализация лишена подобных недостатков. Каждая зона в ней соответствует определенному помещению. Однако такой вариант исполнения обходится дороже на стадии монтажа.

В современных системах пожарной сигнализации вместо пульта используется специальное программное обеспечение.

Блок резервного питания обеспечивает работу пожарной сигнализации в случае отсутствия питания от электросети.

Более продвинутый вариант пожарной сигнализации – система автоматической пожарной сигнализации и пожаротушения (САПСПТ). Она представляет собой совокупность установок и оборудования пожарной сигнализации, управляемую централизовано. На рисунке 3.7

представлена схема части САПСПТ – автоматической пожарной сигнализации.

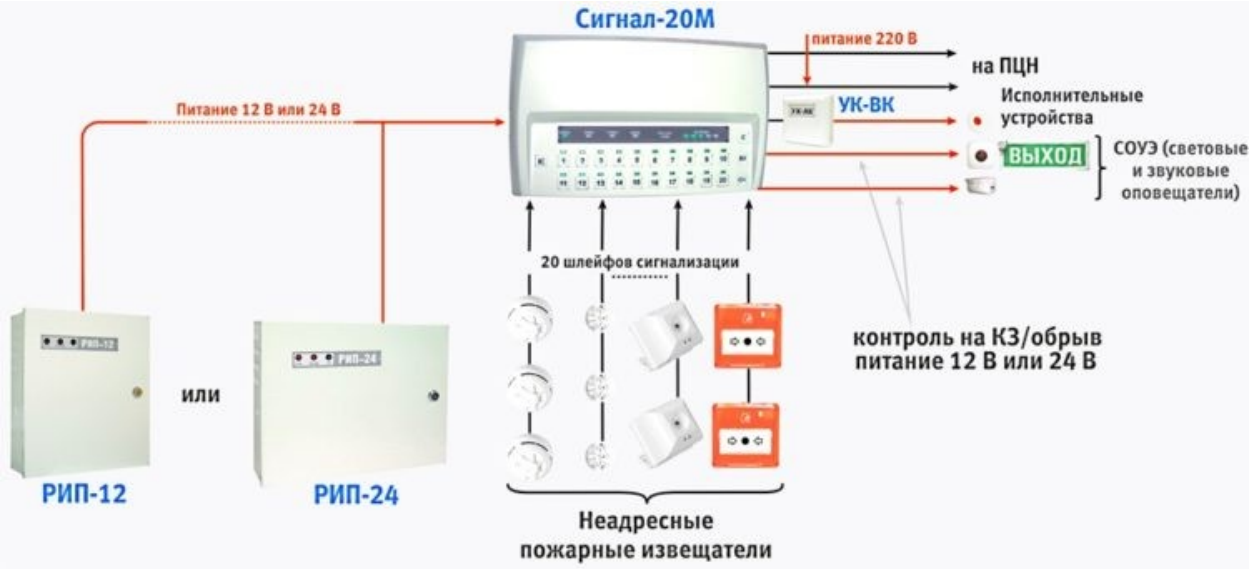

Рис. 3.7 – Структурная схема автоматической пожарной сигнализации в составе САПСПТ

Система автоматического пожаротушения в составе САПСПТ может быть различных типов в зависимости от вида используемых веществ. Выделяют следующие типы систем автоматического пожаротушения:

1. Газовая система. Принцип работы подобной системы основан на том, что используемый газ вытесняет кислород из зоны горения или же создает реакцию с продуктами горения, прекращая сам процесс.

2. Водяная система. Наиболее простая и безвредная для людей система, за счет чего она часто используется в помещениях, предусматривающих массовое скопление людей. Пожар тушится тонкими струями воды. Схема системы водяного пожаротушения дренчерного типа представлена на рисунке 2.14.

3. Аэрозольная система. Данная система безопасна для людей и очень эффективна. При появлении очага возгорания срабатывает пиропатрон и за счет импульса вырабатывается облако реактива, заполняющее помещение и прекращающее пожар. Частицы активного вещества при этом имеют очень маленький размер – до 10 микрон.

4. Порошковая система. Данная система осуществляет тушение порошкообразным реагентом. Она может быть применима в тех помещениях, где недопустимо использовать воду. Например, в местах выработки электроэнергии.

Рис. 3.8 – Схема системы водяного пожаротушения

САПСПТ имеет следующие преимущества перед обычными пожарными сигнализациями:

- низкая вероятность ложного срабатывания;

- процесс тушения пожара максимально автоматизирован;
- очаг возгорания легко определить;
- при помощи программного обеспечения возможна интеграция с другими системами безопасности (например, с системой видеонаблюдения);
- простота в настройке и эксплуатации.

К недостаткам системы можно отнести сложность монтажа и высокую стоимость оборудования.

Охранная сигнализация – важная составляющая системы безопасности. Также, как и пожарная, охранная сигнализация состоит из трех основных компонентов:

- контрольной панели (контроллера);
- датчиков (извещателей);
- оповещателей;
- источника бесперебойного питания;
- пульта управления (АРМ оператора системы).

Примерная схема охранной системы представлена на рисунке 3.9.

Рис. 3.9 – Примерная схема построения охранной сигнализации

Центральным элементом оборудования системы охранной сигнализации является контроллер. К контроллеру подключаются датчики и оповещатели. Подключение может осуществляться как проводами, так и по радиоканалу. Радиоохранные сигнализации разумно использовать на тех объектах, где невозможно провести полноценные строительно-монтажные работы, поскольку проводной способ подключения датчиков всё же является более надежным. Контроллеры могут отличаться количеством доступных охраняемых зон, способом обработки сигнала. Аналоговые контроллеры реагируют только на размыкание цепи на шлейфе, к которому подключен датчик. Аналоговые контроллеры, как правило, не предусматривают точную адресацию. Точность срабатывания датчиков ограничивается охраняемой зоной, которая может включать несколько помещений. Цифровые контроллеры взаимодействуют с каждым датчиком по своему каналу связи, производя его опрос. Их невозможно обмануть подменой устройства или принудительным замыканием цепи. Цифровым контроллерам присуща адресность до уровня датчика.

Датчики располагаются по всей охраняемой территории. При срабатывании датчика в зависимости от настроек производится оповещение о проникновении при помощи используемых оповещателей.

Существуют следующие типы датчиков:

1. Инфракрасный датчик движения. Принцип работы таких датчиков основан на фиксации изменения окружающей обстановки в инфракрасном диапазоне. Активные датчики контролируют излучаемые ими лучи и фиксируют факт пересечения хотя бы одного из них. Пассивные контролируют изменения инфракрасного фона в охраняемой области, разделяемой на сектора. Перемещение в охраняемой зоне любого объекта, излучающего или поглощающего тепло, вызывает срабатывание датчика.

2. Ультразвуковой датчик движения. Данный датчик работает за счет анализа звуковых волн из диапазона выше человеческого восприятия. Излучатель внутри датчика испускает пучки ультразвуковых волн, после чего приемник ловит отраженные сигналы. Если изменения в охраняемой области отсутствуют, волны всегда возвращаются одинаково.

3. Радиоволновой датчик движения. Принцип работы радиоволного датчика схож с ультразвуковым, но для анализа среды используются радиоволны. В отличие от акустических, радиоволны способны проникать через предметы, состоящие из полупроводников и изоляторов. Данный тип датчиков используется достаточно редко из-за своей дороговизны.

4. Фотоэлектрический датчик движения. В датчиках подобного типа используется принцип проверки прерывания светового потока, поэтому датчик физически состоит из двух частей. Излучатель испускает световой поток, а приемник принимает. На светочувствительной пластинке приемника под действием света возникает фототок. Соответственно, отсутствие светового луча размыкает электрическую цепь и датчик срабатывает.

5. Акустический датчик разбития стекла. Принцип действия акустических датчиков построен на фиксации звуковых волн из диапазона, различаемого человеком. Для фиксации звука используется микрофон, преобразующий акустический сигнал в электрический

6. Вибрационный датчик разбития стекла/пролома двери. Данный тип датчика при помощи тензорезисторов улавливает вибрацию, которая может возникать при проломе или выпиливании конструкции, а также при разбитии стекла. Поскольку акустические датчики значительно проще и дешевле, вибрационные датчики для обнаружения разбития стекла, как правило, не используются.

7. Магнитоконтактные датчики открытия дверей и окон. Очень простой и эффективный тип датчиков, предназначенный для определения факта открытия окон, дверей, ворот, люков. Физический магнитоконтактный датчик состоит из двух частей: геркона и магнита. Если обе части датчика находятся в непосредственной близости, контакты замкнуты. При удалении одной части датчика от другой на критическое расстояние контакты размыкаются и вызывают срабатывание датчика

Оповещатели охранной сигнализации могут быть звуковыми и световыми. В отличие от пожарной сигнализации срабатывание датчиков охранной сигнализации не обязательно предусматривает громкое звуковое и яркое световое оповещение. Данный момент определяется целями действий в отношении злоумышленника: спугнуть и прекратить выполнение противоправного действия или же задержать до появления сотрудников правоохранительных органов. Первоочередной

задачей является уведомление уполномоченных сотрудников организации тем или иным способом (звуковое, световое, текстовое). Современные системы охранной сигнализации способны уведомлять о срабатывании датчиков путем отправки письма на электронную почту или СМС-сообщения.

Источник бесперебойного питания предназначены для обеспечения функционирования системы охранной сигнализации при обесточивании охраняемых зон. При переходе на резервное питание система охранной сигнализации должна уведомить об этом уполномоченных сотрудников предприятия при помощи оповещателей.

При помощи пульта управления оператор может настраивать систему охранной сигнализации, ставить помещения под охрану и наблюдать срабатывание датчиков в охраняемых зонах. Многие современные системы охранной сигнализации могут управляться помощи специального программного обеспечения, что дает возможности для интеграции с другими системами безопасности, например, с системой видеонаблюдения.

Система видеонаблюдения является важным компонентом решения задачи по обеспечению безопасности, сохранности материальных ценностей и контроля работы сотрудников. Можно сформировать типовой список целей, с которыми обычно устанавливается система видеонаблюдения:

- охрана территории предприятия от проникновения посторонних;
- постоянный визуальный контроль основных бизнес-процессов предприятия;
- обеспечение защиты материальных ценностей;

- фиксация перемещения товаров, грузов, продукции, документации;
- контроль въезда/выезда на охраняемую территорию транспортных средств;
- контроль работы автоматического оборудования;
- контроль соблюдения сотрудниками предприятия техники безопасности;
- контроль за дисциплиной труда;
- решение внештатных ситуаций;
- получение материала для служебных расследований.

При построении системы видеонаблюдения необходимо учитывать множество факторов: особенности территории, расположения контролируемых объектов, условий монтажа, возможностей обеспечения электропитания, технических условий работы оборудования и т.д. Построение обычно начинают со схемы видеонаблюдения, отображающей зоны покрытия видеонаблюдения. Пример такой схемы представлен на рисунке 3.10.

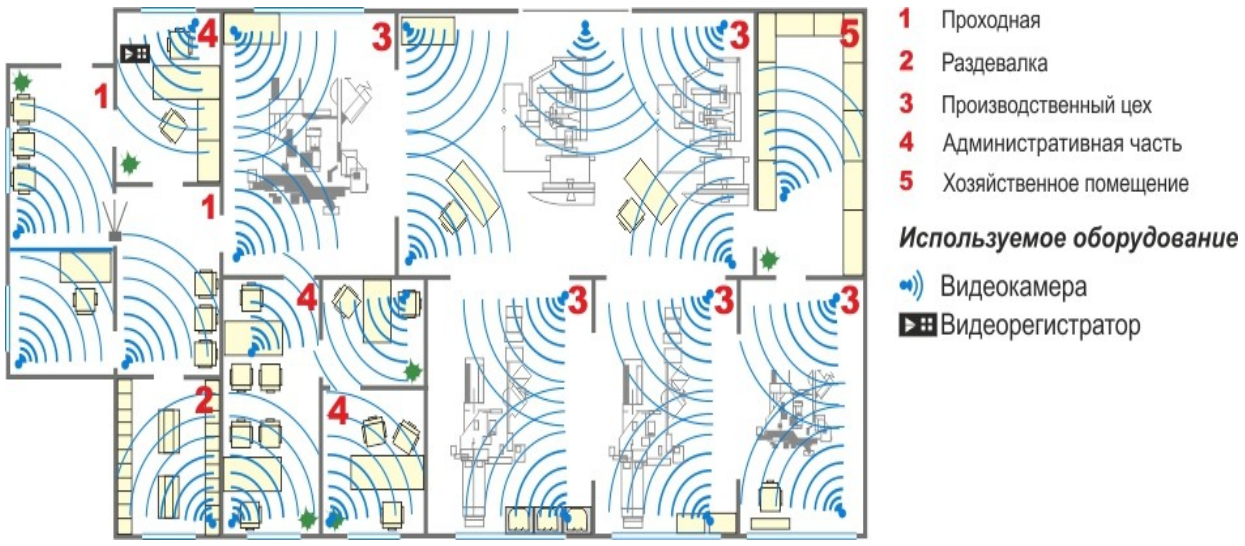

Рис. 3.10 – Схема видеонаблюдения с указанием зон покрытия видеокамер

Иногда для дополнительной визуализации используется трехмерное моделирование (см. рисунок 3.11).

Рис. 3.11 – Трехмерная визуализация системы наблюдения

Структурно система видеонаблюдения состоит из видеорегистратора и видеокамер.

Видеорегистраторы бывают сетевыми, аналоговыми и гибридными. Выбор типа видеорегистратора зависит от типа планируемых к покупке камер. Если необходимо обеспечить хорошую управляемость и масштабируемость, рекомендуется

использовать сетевой видеорегистратор. Однако это увеличит затраты на систему видеонаблюдения и создает риски получения несанкционированного доступа к камерам через локальную сеть предприятия. Также при выборе видеорегистратора следует обратить внимание на следующие параметры:

- разрешение изображения;
- скорость записи;
- поддерживаемый объем накопителей для записи;
- количество каналов записи;
- возможность записи звука;
- возможность подключения поворотных камер;
- многозадачность.

Вместо регистратора для IP-камер допустимо использовать видеосервер – компьютер с установленными программным обеспечением для записи и просмотра видео.

Видеокамеры классифицируются по следующим параметрам:

1. Физический тип подключения (проводной или беспроводной). Проводное соединение надежнее, но требует затрат на монтаж.

2. Тип передаваемого сигнала (аналоговый или цифровой). Цифровая передача данных обеспечивает более высокое качество картинки, удобное управление архивом видеозаписей, возможность масштабировать изображения. Также беспроводная передача данных в представленных на рынке видеонаблюдения решениях доступна только в цифровом виде.

3. Место установки (внутренние или внешние). Внутренние камеры более легкие и на первое место в них

выходит качество изображения. Внешние камеры предназначены для работы в менее благоприятных средах, поэтому их класс защиты значительно выше. Внешние камеры допустимо устанавливать во внутренних помещениях, когда это оправдано повышенной агрессивностью среды. Например, внешние камеры устанавливают в цехах производственных предприятий с повышенной влажностью и/ или пониженной температурой.

4. Статичность (неподвижные или поворотные). Неподвижные камеры фиксируются креплениями при монтаже и их зона обзора не меняется. Поворотные камеры позволяют дистанционно управлять своей зоной обзора за счет поворота объектива на заданный угол.

5. Угол обзора. Данный параметр весьма неоднозначен. Чем больше это значение, тем больший угол обзора обеспечивает камера, но тем больше искажение и меньше фокусное расстояние. Для ясности необходимо рассмотреть этот момент с точки зрения законов оптики.

Фокусное расстояние – дистанция между оптическим центром объектива и его главным фокусом. Главный фокус – точка, в которой собирается пучок света, распространяющийся вдоль главной оптической оси. При условии, что наблюдаемый объект полностью попадает в поле зрение объектива камеры по высоте, фокусное расстояние можно рассчитать следующим образом:

$$f = \frac{v * D}{V} (4)$$

где:

- v – высота матрицы объектива в миллиметрах;
- D – реальное расстояние до наблюдаемого объекта;

- V – высота объекта.

Чем больше фокусное расстояние – тем выше детализация и тем меньше угол обзора. Также верно и обратное утверждение. Для упрощения оценки требований к детализации применяются следующие абстракции:

- зона наблюдения (объект занимает от 25 до 30% высоты экрана, различаются характерные детали объекта);
- зона узнавания (объект занимает не мене 50% высоты экрана, можно определить, появлялся ли он в зоне наблюдения ранее);
- зона идентификации (объект занимает не менее 100% высоты экрана, качества изображения и детализации достаточно для однозначного установления личности) [26].

Необходимо определить требуемое расстояние для каждой из этих зон в каждой точке наблюдения и выбирать фокусное расстояние камеры, исходя из рассчитанных данных

6. Форм-фактор (обычные, купольные, миникамеры). В зависимости от целей и задач наблюдения можно выбрать камеры в различных корпусах. Решающими факторами здесь могут быть требуемая заметность камер и требования к дизайну.

7. Наличие инфракрасной подсветки. Камера, обладающая инфракрасной подсветкой, способна давать качественную картинку в темное время суток.

Для того, чтобы вышеописанное аппаратное обеспечение могло работать друг с другом, а также для обеспечения потоков информации между различными системами безопасности и информационной системой

предприятия, необходимо различное программное обеспечение.

3.3 Необходимое программное обеспечение системы защиты информации

Современные устройства локальной сети обладают своим программным обеспечением (зачастую даже операционной системой) для обеспечения требуемого функционала. Однако для обеспечения сетевой безопасности серверов и рабочих станций требуется дополнительное программное обеспечение:

1. Брандмауэр или сетевой экран. Это программное обеспечение для контроля и фильтрации проходящего через сетевой интерфейс трафика в соответствии с настроенными правилами. Правила могут быть настроены по следующим критериями:

- фильтрация по IP-адресу основана на IP-адресе отправителя пакета, указанного в заголовку;
- фильтрация по доменному имени аналогично фильтрации по IP-адресу, за исключением того, что в качестве идентификатора используется доменное имя отправителя пакета;
- фильтрация по портам основывается на адресах портов отправителя и получателя;
- фильтрация по протоколам работает следующим образом: файрвол разбирает заголовки сетевых пакетов и определяет тип используемого протокола.

Сетевой экран может работать с 3 по 7 уровни модели ISO/OSI (см. рисунок 3.12).

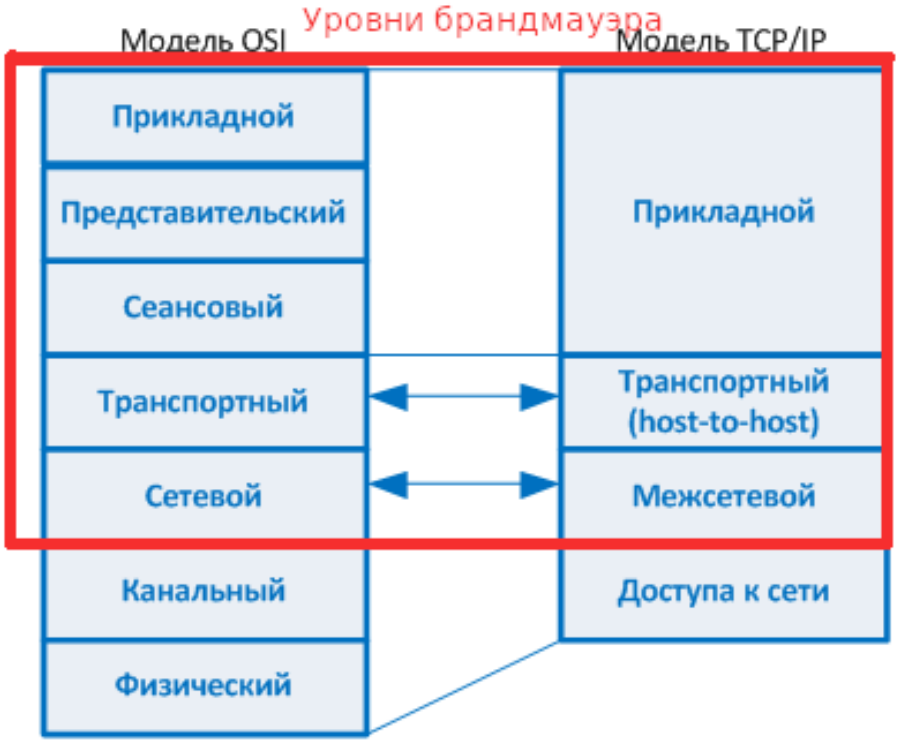

Рис. 2.18 – Уровни работы брандмауэра

Следует заметить, что фильтрация на отмеченных прикладнос, представительском и сеансовом уровнях недостижима путем простого анализа пакетов. Необходим более детальный анализ проходящих через сетевой интерфейс пакетов по технологии DeepPacketInspection (DPI). Её суть в анализе пакета как по статическим паттернам, так и по поведенческим признакам, что позволяет распознать даже те приложения, которые не используют предопределенные последовательности и структуры данных. Подобный анализ схож с эвристическим анализом антивирусных программ, однако современный анализ пакетов может использовать не только четкие алгоритмы, но и технологию машинного обучения (нейросети).

2. Системы обнаружения и предотвращения вторжений. Для реализации комплексного подхода к защите к локальной сети используются системы обнаружения и предотвращения вторжений (СОПВ). Под СОПВ обычно понимают программное обеспечение, которое способно выявить факты несанкционированного доступа к локальной сети или информационным ресурсам предприятия. СОПВ позволяют обнаружить подозрительную активность, которая потенциально угрожает безопасности информационной системы. Активность может выражаться в виде сетевых атак на сервисы, атак с целью повышения привилегий, несанкционированного доступа к защищаемой информации или действий вредоносного программного обеспечения.

СОПВ структурно состоит из следующих компонентов:

- сенсорной подсистемы;
- аналитической подсистемы;
- базы данных событий и результатов работы аналитической подсистемы;
- консоли управления.

В простых СОПВ все перечисленные части системы обычно реализованы в одном модуле.

Существуют четыре основных типа СОПВ [16]:

- сетевые СОПВ, осуществляющие обнаружение вторжений путем отслеживания внутрисетевого трафика (доступ к трафику может осуществляться через коммутатор, поддерживающий зеркалирование портов);

- СОПВ, основанные на конкретном протоколе коммуникации (система, производящая анализ коммуникационных протоколов между узлами локальной сети);

- СОПВ, основанные на конкретном протоколе (система, производящая анализ коммуникационных протоколов между узлами локальной сети);
- СОПВ, основанные на прикладных протоколах – программное обеспечение, отслеживающее данные, передаваемые по протоколам, специфичными для конкретных приложений;
- узловые СОПВ (наблюдают и анализируют системные вызовы, журналы приложений, файловые дескрипторы);
- гибридные СОПВ, совмещающие в себе несколько подходов из перечисленных выше.

Также СОПВ подразделяются на активные и пассивные. Пассивные СОПВ нацелены на обнаружение вторжения, фиксацию этого факта и технической информации, а также уведомления ответственного сотрудника. Активные СОПВ действуют тем же образом, что и пассивные, но при обнаружении вторжения они пытаются противодействовать нарушителю, разрывая соединения или динамически корректируя настройки брандмауэра.

3. Средства предотвращения утечек информации. Серьезной угрозой для информационной безопасности предприятия являются утечки конфиденциальной информации и информации для служебного пользования, которые происходят по вине сотрудников. Согласно статистике, от 80% до 95% всех утечек случаются из-за корпоративных пользователей. Действия (или бездействие) сотрудников, приводящие к данной проблеме, могут быть как намеренными, так и неосознанными. Передача информации может быть осуществлена как посредством доступа в сеть

Интернет, так и при помощи съемных носителей. Безусловно, частично можно решить данную проблему при помощи настройки сетевого экрана и программного запрета на подключение внешних носителей, но для глобального решения вопроса на средних и крупных предприятиях рекомендуется внедрять системы защиты от утечек информации.

Системы защиты от утечек информации (СЗУИ) открывают перед организацией следующие возможности:

- создание политик передачи информации внутри предприятия, а также входа и выхода информации за его пределы;
- категоризация информации по степени конфиденциальности;
- осуществление контроля за движением информации в течение всего жизненного цикла (хранение, обработка, передача);
- обнаружение копий защищенной информации за пределами специально организованных для хранения ресурсов;
- уведомление ответственного сотрудника (и при необходимости сотрудника-нарушителя) о факте нарушения политики информационной безопасности предприятия;
- централизованный контроль и управление системой.

Еще одной немаловажной проблемой является конфиденциальность данных на корпоративных мобильных устройствах [17]. Утеря или кража устройства может привести к таким негативным последствиям как компрометация учетных данных, разглашение

конфиденциальной информации или раскрытие персональных данных. Системы защиты мобильных устройств, предназначенные специально для этих целей, позволяют не только снизить риски утечки защищаемой информации но и уменьшить потенциальный эффект от утечки. Как правило, они обладают следующими возможностями:

- шифрование данных в памяти устройства;
- использование средств двухфакторной аутентификации;
- централизованное управление учетными данными и разграничением прав пользователей;
- автоматическая проверка устройств на предмет вредоносного программного обеспечения;
- дистанционная блокировка устройства и очистка его памяти в случае утери или кражи.

Совокупность систем защиты от утечек информации используется в технологии DLP (DataLeakagePrevention, - предотвращение утечки данных). Именно эта технология в настоящее время считается наиболее рекомендованной к внедрению на средних и крупных предприятиях. Система DLP должна контролировать и при необходимости блокировать передачу данных посредством любого интерфейса компьютера. Исключениями является фото- и видеосъемка экранов компьютеров пользователей, а также побочное электромагнитное излучение наводки, для борьбы с которыми необходимо прибегать к дорогим техническим средствам.

Современные системы управления контроля доступом также предусматривают использование программного обеспечения. Безусловно, небольшие организации могут

позволить себе настройку доступа на каждом контроллере, но для средних и крупных требуется централизованное управление. Программное обеспечение контроля доступа – комплекс программных продуктов, позволяющий обеспечить надежность эксплуатации СКУД, а также обладающее следующей функциональностью:

- управление доступами и идентификаторами пользователей;
- определение характеристик точек доступа;
- мониторинг и логирование событий доступа;
- интеграция с другими информационными системами предприятия.

Структурно программный комплекс для СКУД может состоять из некоторого количества модулей (в программном обеспечении от различных разработчиков структура может несколько варьироваться) [20]:

1. Система управления базами данных (СУБД). Этот модуль всегда является сторонним. Выбор СУБД, как правило, зависит от тех или иных предпочтении разработчика программного комплекса. СУБД может быть как свободным, так и проприетарным программным обеспечением.

2. Программа конфигурирования и тестирования комплекса. Данный компонент используется при внедрении всего программного комплекса для отладки и тестирования, а также вноса базовой конфигурации (тех настроек, которые вводятся только один раз – количество контроллеров, дверей, схема их местоположения)..

3. Программа настройки СКУД. С помощью данного программного обеспечения конфигурируются полномочия

сотрудников безопасности и профили пользователей системы (зоны доступа, двери, графики посещения).

4. Основная программа СКУД. Этот компонент отвечает за общее управление другими элементами СКУД.

5. Базовый модуль СКУД. Это программное обеспечение решает задачи управления пользователями (добавление, изменение, удаление, установка связи с идентификаторами, назначение разрешенных зон прохода, ведение журналов)

6. Модуль поддержки планов объектов. Данный компонент обеспечивает визуализацию устройств СКУД на плане здания, а также адресное отображение событий, обеспечивает масштабируемость планов.

7. Модуль выдачи идентификаторов СКУД. Учетный модуль, позволяющий вести журнал учета посетителей, заявок на выдачу идентификаторов, а также обеспечивающий оформление выдачи идентификаторов.

8. Программа учета рабочего времени. Позволяет учитывать рабочее время сотрудников на основании данных о проходе в определенные зоны или помещения. Может интегрироваться с другими информационными системами предприятия (например, 1С: Предприятие 8. Зарплата и кадры).

9. Модуль «Электронная проходная». Модуль обеспечивает вывод на АРМ охранника фотографии, ФИО, должности и других данных, привязанных к считанному идентификатору.

10. Модуль «Правила». Модуль расширяет возможности СКУД логическими условиями (запрет

повторного прохода, шлюзовый проход, разблокировка замков по времени и др.).

11. Модули интеграции. Программное обеспечение СКУД может интегрироваться как с другими системами безопасности (видеонаблюдением, пожарной и охранной сигнализациями), так и с учетными системами предприятия.

Программное обеспечение системы охранно-пожарной сигнализации предназначено для решения следующих задач:

- централизованное управление приборами;
- удаленный сбор информации о техническом состоянии контроллеров и датчиков и вывод информации о необходимости замены;
- интеграция с другими охранными системами.

Программное обеспечение системы видеонаблюдения, как правило, используется для реализации видеосерверов для IP-камер вместо аппаратных видеорегистраторов. Подобная система организации видеонаблюдения позволяет лучше управлять архивами записей и успешно интегрировать видеонаблюдения с другими охранными и информационными системами предприятия.

Выводы по разделу:

В практической части описана предложенная методика разработки плана модернизации системы информационной безопасности предприятия. Также в разделе рассмотрены принципы подбора необходимого аппаратного и программного обеспечения для построения комплексной системы защиты информации. Таким образом, заявленные во введении задачи были полностью выполнены в рамках данной выпускной квалификационной работы.

ЗАКЛЮЧЕНИЕ

В данной выпускной квалификационной работе была произведена разработка методологии модернизации системы информационной безопасности предприятия. Базой для выполнения работы являлась производственная преддипломная практика, пройденная на предприятии ООО «Каскад».

В первой главе работы рассмотрены теоретические основы решаемой проблемы, а именно:

- определены основные угрозы информационной безопасности малых, средних и крупных предприятий
- проанализированы современные подходы к анализу существующих систем информационной безопасности предприятий
- изучены этапы процесса модернизации системы информационной безопасности предприятия.

Вторая глава работы посвящена характеристике предприятия, обобщенному анализу модели угроз. В ней рассмотрены типовые проблемы существующих систем информационной безопасности, методы их решения, проанализированы особенности формирования концепции и политик информационной безопасности.

В третьей главе работы описаны следующие практические аспекты исследования:

- разработка плана модернизации системы информационной безопасности;
- подбор необходимого аппаратного обеспечения системы защиты информации;

- подбор необходимого программного обеспечения системы защиты информации.

В процессе выполнения работы были полностью выполнены задачи, поставленные во введении и достигнута основная цель работы: разработка методологии модернизации системы информационной безопасности предприятия.

СПИСОК ИСПОЛЬЗОВАННЫХ ИСТОЧНИКОВ

1. ГОСТ Р ИСО/МЭК 15408-1-2008 «Методы и средства обеспечения безопасности. критерии оценки безопасности информационных технологий».

2. ГОСТ Р 51275-2006 Защита информации. Объект информатизации. Факторы, воздействующие на информацию. Общие положения.

3. Бабаш, А.В. Информационная безопасность. История защиты информации в России / А.В. Бабаш, Е.К. Баранова, Д.А. Ларин – КДУ, 2015 – 736 с.

4. Бабаш, А.В. Информационная безопасность. Практикум / А.В. Бабаш, Е.К. Баранова, Ю.Н. Мельников – М: КноРус, 2017 – 349 с.

5. Басыня, Е.А. Сетевая информационная безопасность и анонимизация / Е.А. Басыня – НГТУ, 206 – 342 с.

6. Басыня, Е.А. Системное администрирование и информационная безопасность / Е.А Басыня – НГТУ, 2016 – 265 с.

7. Бахарев, С. Безопасность объектов энергетического комплекса / Сергей Бахарев. - М.: LAP LambertAcademicPublishing, 2016. - 384 с

8. Бахаров, Л.Е. Информационная безопасность и защита информации / Л.Е. Бахаров – М: НИТУ МИСиС, 2016 – 345 с

9. Бирюков, А.А. Информационная безопасность. Защита и нападение / А.А. Бирюков – СПБ: ДМК Пресс, 2017 – 550 с.

10. Галкин, А. Информационная безопасность и целесообразные пути ее улучшения / А. Галкин – М: КноРус, 2016 – 80 с.

11. Гришина, Н.В. Информационная безопасность предприятия. Учебное пособие / Н.В. Гришина – М: Форум, 2019 – 240 с.

12. Груба, М.И. Системы охранной сигнализации. Технические средства обнаружения / М.И. Груба – М:Солрн-Пресс, 2012 – 220 с.

13. Дождиков, В.Г. Информационная безопасность. Национальные стандарты Российской Федерации. Учебное пособие / В.Г. Дождиков – М: LAP LambertAcademicPublishing, 2015 – 240 с.

14. Ефимов, Л.Л. Информационная безопасность детей. Российский и зарубежный опыт / Л.Л. Ефимов, С.А. Кочерга – Юнити-Данта, 2014 – 240 с.

15. Корниенко Б. Информационная безопасность и технологии компьютерных сетей / Б. Корниенко – М: КноРус, 2017 – 112 с.

16. Коршаковский, С. Неразрушающий контроль и безопасность в энергоёмких объектах техники / Станислав Коршаковский. - М.: LAP LambertAcademicPublishing, 2018. - 424 с.

17. Косовец А.А. Информационные технологии и информационная безопасность в системе государственного управления / А.А. Косовец – Издательский дом Университета «Синергия», 2017 – 452 с.

18. Курбатов В.А. Политики информационной безопасности / В.А. Курбатов, С.А. Петренко – М: КноРус, 2018 – 400 с.

19. Лазарев, И.А Информация и безопасность. Композиционная технология информационного моделирования сложных объектов принятия решений / И.А Лазарев. - М.: Московский городской центр научно-технической информации, 2016. - 336 с.

20. Майоров, А.В. Безопасность функционирования автоматизированных объектов / А.В. Майоров, Г.Н. Москатов, Г.П. Шибанов. - М.: Машиностроение, 2018. - 264 с.

21. Махутов, Н.А. Безопасность России. Правовые, социально-экономические и научно-технические аспекты. Том 2: Безопасность и защищенность критически важных объектов. Часть 1 / Н.А. Махутов. - М.: Знание, 2016. - 382 с.

22. Махутов, Н.А. Безопасность России. Правовые, социально-экономические и научно-технические аспекты. Том 2: Безопасность и защищенность критически важных объектов. Часть 2 / Н.А. Махутов. - М.: Знание, 2018. - 412 с.

23. Медведев, В.А. Информационная безопасность. Введение в специальность. Учебник / В.А. Медведев – М: КноРус, 2019 –144 с.

24. Мельников, В.П. Информационная безопасность / В.П. Мельников, А.И. Куприянов – М: КноРус, 2015 – 323 с.

25. Мельников, В.А. Информационная безопасность открытых систем / В.А. Мельников – Флинта, 2017 – 413 с.

26. Михайлов, Ю.Б. Научно-методические основы обеспечения безопасности защищаемых объектов / Михайлов Юрий Борисович. - М.: Горячая линия - Телеком, 2016. - 350 с.

27. Мытник, К.Я. Смарт-карты и информационная безопасность / К.Я. Мытник, С.П. Панасенко – ДМК Пресс, 2018 – 415 с.

28. Нестеров, С.А. Основы информационной безопасности. Учебное пособие / С.А. Нестеров – СПБ: Лань, 2016 – 324 с.

29. Оноприенко, М. Г. Безопасность жизнедеятельности. Защита территорий и объектов экономики в чрезвычайных ситуациях. Учебное пособие / М.Г. Оноприенко. - М.: Дрофа, 2018. - 400 с.

30. Оноприенко, М.Г. Безопасность жизнедеятельности. Защита территорий и объектов экономики в чрезвычайных ситуациях: Учебное пособие / М.Г. Оноприенко. - М.: Форум, 2018. - 288 с.

31. Петренко, С.А. Политики безопасности компании при работе в Интернет / С.А. Петренко, В.А. Курбатов – СПБ: БХВ-Петербург, 2010 – 400 с.

32. Петров, В.П. Информационная безопасность человека и общества: учебное пособие / В.П. Петров, С.В. Петров – Энас, 2015 – 353 с.

33. Родичев, Ю.А. Информационная безопасность. Национальные стандарты Российской Федерации. Учебное пособие / Ю.А. Родичев – СПБ:Питер, 2019 – 304 с.

34. Родичев, Ю.А. Информационная безопасность: нормативно-правовые аспекты / Ю.А. Родичев – СПБ: Питер, 2017 – 345 с.

35. Собурь, С.В. Краткий курс пожарно-технического минимума / С.В. Собурь – М: Пожарная книга, 2012 – 288 с.

36. Ушаков, В. Обеспечение безопасности объектов. Физическая защита / Владимир Ушаков. - М.: Издательские решения, 2019. - 431 с.

37. Цветков В. Информационная безопасность ГИС и инфраструктуры / В. Цветков, С. Булгаков – М: КноРус, 2017 – 156 с.

38. Шаньгин, В.Ф. Информационная безопасность и защита информации / В.Ф. Шаньгин – ДМК Пресс, 2017 – 702 с.

39. Шунейко, А.А. Информационная безопасность человека / А.А. Шунейко, И.А. Авдеенко – Владос, 2018 – 563 с.