СОДЕРЖАНИЕ

ВВЕДЕНИЕ

В соответствии с учебным планом была пройдена учебная практика с «09» февраля 2023г. по «31» мая 2023г по теме «Модель защиты информационных ресурсов на предприятии».

Тема защиты информационных ресурсов предприятия была выбрана из-за её актуальности на данный момент. Доктрина информационной безопасности Российской Федерации, среди прочих, выделяет следующие информационные угрозы для РФ

1. Ряд западных стран наращивает возможности информационно-технического воздействия на информационную инфраструктуру в военных целях.
2. Усиливается деятельность организаций, осуществляющих техническую разведку в России.
3. Возрастают масштабы компьютерной преступности, прежде всего в кредитно-финансовой сфере.
4. Растет число преступлений, связанных с нарушением конституционных прав и свобод человека, неприкосновенности частной жизни, защиты персональных данных. Эти преступления становятся все изощреннее.
5. Иностранные государства усиливают разведывательную деятельность в России. Растет количество компьютерных атак на объекты критической информационной инфраструктуры, их масштабы и сложность растут.

Исходя из вышеназванных пунктов, можно утверждать, что защита информационных ресурсов на всех возможных уровнях, в том числе и на предприятиях, как критической, так и частной инфраструктуры, является приоритетной областью развития Российской Федерации в области информационной безопасности.

1 ОБЩИЕ ПОЛОЖЕНИЯ ЗАЩИТЫ ИНФОРМАЦИИ

Перед ознакомлением с положениями защиты информации, следует определить само понятие «защита информации». Под защитой информации подразумевается деятельность, направленная на предотвращение утечки защищаемой информации, несанкционированных и непреднамеренных воздействий на защищаемую информацию. В свою очередь, защита информации подразделяется на виды защиты (рис.1) и способы защиты (рис.2) информации.

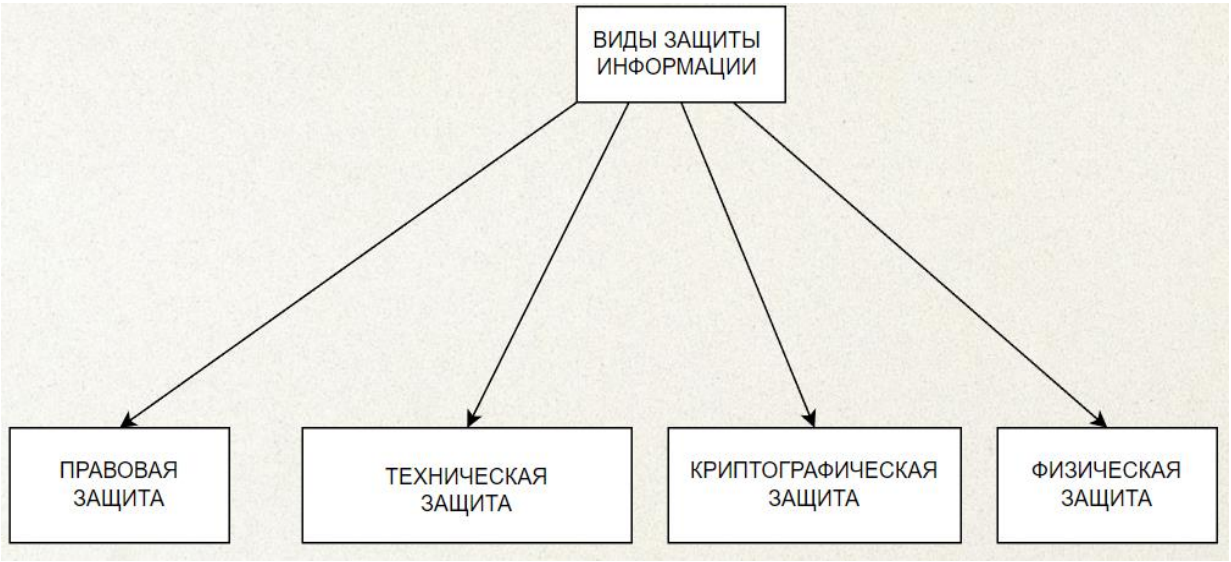

Рисунок 1. Виды защиты информации

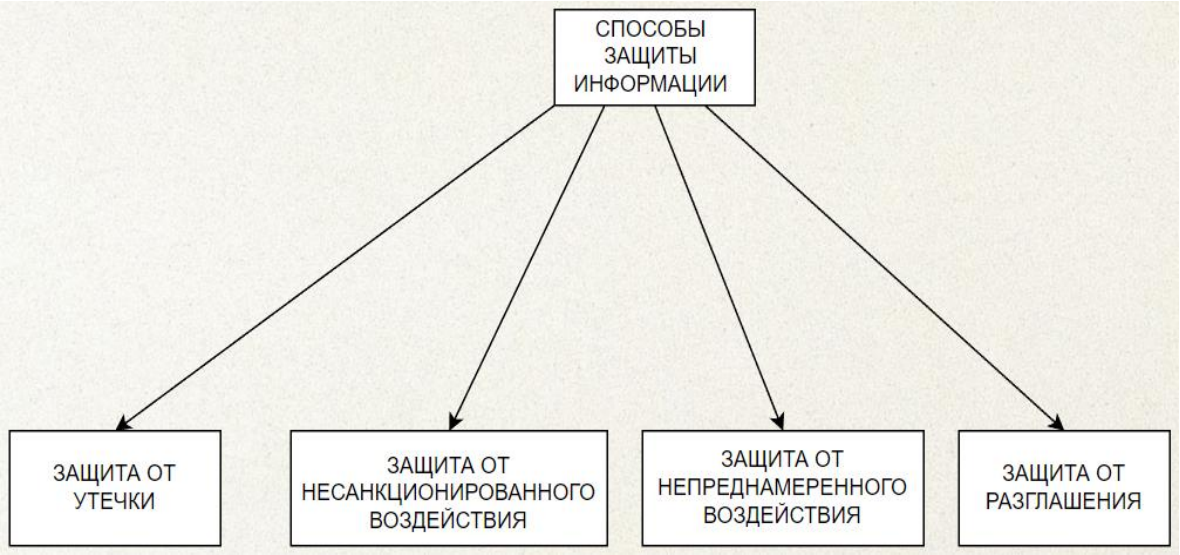

Рисунок 2. Способы защиты информации

Разделение на виды, и реализация в каждом виде доступных способов формируют понятие информационной безопасности информации (ИБ). Под информационной безопасностью подразумевается состояние информационной системы, в котором обеспечивается защита информации и поддерживающей её инфраструктуры от естественных и искусственных угроз (рис.3).

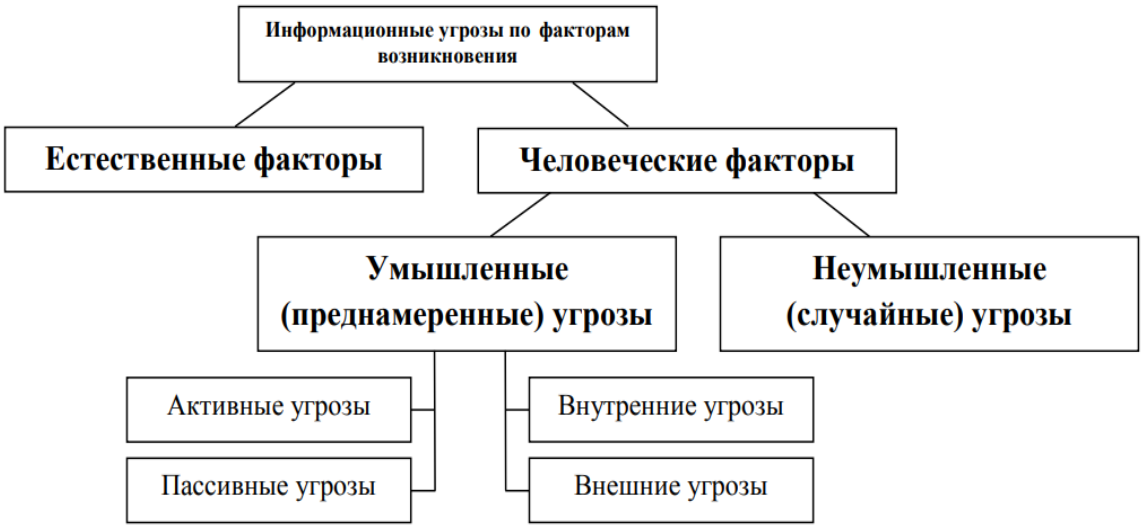

Рисунок 3. Угрозы информационной безопасности

2 УГРОЗЫ ИНФОРМАЦИОННОЙ БЕЗОПАСНОСТИ

В контексте информационных систем, угрозой информационной безопасности считают совокупность условий, факторов и действий, направленных на нарушение работоспособности информационной системы или свойств информации (целостность, доступность, конфиденциальность).

При более конкретном рассмотрении можно разделить все угрозы ИБ на:

1. Угрозы для государства.
2. Угрозы для предприятия.
3. Угрозы для частного лица.

К угрозам предприятия можно отнести:

1. Разглашение - умышленные или неосторожные действия должностных лиц или пользователей информации, которым она была доверена в соответствующем порядке, и действия которых привели к ознакомлению с информацией лиц, к этой информации не допущенных.

2. Утечку- бесконтрольный выход конфиденциальной информации за пределы организации или круга лиц, которым она была доверена.

3. Несанкционированный доступ- противоправное ознакомление с конфиденциальной информацией лиц, не имеющих к ней доступа.

4. Естественные угрозы (стихийные бедствия-пожары, наводнения, землетрясения и другие причины).

2.1 Несанкционированный доступ

Несанкционированный доступ (НСД) является самой частой угрозой информационной безопасности. Одной из главных проблем, встречающихся на предприятиях, является разделение доступа к информации у сотрудников. Другими словами, службе безопасности необходимо определить какие данные для какого сотрудника являются конфиденциальными. По характеру воздействия (рис.2) НСД является активным воздействием на информационную систему, использующим её уязвимости. Злоумышленник,

используя НСД воздействует либо на требуемую информацию, либо на информацию о санкционируемом доступе с целью легализации НСД. НСД может быть осуществлен с помощью:

1. Хищения носителей информации и документальных отходов;
2. Инициативного сотрудничества;
3. Склонения к сотрудничеству со стороны взломщика;
4. Выпытывание;
5. Прослушивание;
6. Наблюдение.

2.2 Разглашение и утечка

Разглашение и утечка являются следствием внутренних разногласий в коллективе, малой осведомленности сотрудников о информационной безопасности, использования несертифицированных средств обработки конфиденциальной информации, слабого контроля за соблюдением правил защиты информации. Злоумышленники зачастую пользуются низкими личностно-профессиональными качествами сотрудников фирмы для реализации угроз информационной безопасности. Примеры таких качеств показаны на рисунке 4.

Рисунок 4. Реализация угрозы путем использования личностно-профессиональных недостатков

В то же время, злоумышленники для получения доступа к конфиденциальной информации могут использовать:

1. Визуально-оптические средства (бинокль, телескоп);
2. Акустические (и акустико-преобразовательные) средства;
3. Электромагнитные средства;
4. Материально-вещественные средства (фотографии, документы и т.д.).

Использование данных средств может привести к утечке информации и серьезным финансовым и репутационным потерям для предприятия.

3 ОБЪЕКТЫ И МЕТОДЫ ЗАЩИТЫ ИНФОРМАЦИИ

На основе списка угроз информационной безопасности были разработаны методы защиты информации, применимые к объектам защиты.
К объектам, в отношении которых, требуется осуществлять защиту относятся:

1. Информация - сведения (сообщения, данные) независимо от формы их представления.
2. Носитель информации - физическое лицо или материальный объект, в том числе физическое поле, в котором информация находит свое отражение в виде символов, образов, сигналов, технических решений и процессов, количественных характеристик физических величин.
3. Информационный процесс - процесс создания, сбора, преобразования, накопления, хранения, поиска, распространения, предоставления и использования информации.

Для осуществления защиты информации используется ряд методов. К ним относятся:

1. Идентификация и аутентификация;
2. Проверка прав доступа субъекта к объекту защиты;
3. Мониторинг действий субъекта;
4. Криптографическая защита.

Вместе, данные методы, образуют серьезные преграды для злоумышленника, стремящегося нарушить информационную безопасность системы. Рассмотрим по отдельности вышеперечисленные методы.

Идентификация и аутентификация пользователей- самый первый уровень защиты информации. Идентификация-это процесс выделения конкретного субъекта из общего множества, а аутентификация – подтверждение субъектом факта того, что он является тем, кем представился системе. Эти две операции зачастую выполняются одновременно и позволяют пользователю получить доступ к системе. Самыми простыми примерами идентификатора и аутентификатора являются логин и пароль. В качестве

идентификаторов и аутентификаторов пользователей могут использоваться съемные носители информации (флешки-ключи, магнитные карты и др.), электронные жетоны, механические ключи.

После идентификации и аутентификации субъекта проверяется права доступа субъекта к объекту защиты. Идентификатор и аутентификатор пользователя заносится в журнал мониторинга. Для обеспечения защиты в журнал аудита должны заноситься:

1 Попытки авторизации и деавторизации пользователей в системе;

2 Попытки изменения списка пользователей системы;

3 Попытки изменения политики безопасности системы.

При успешной авторизации пользователь получает доступ к информации, занесенной в систему. В системе информация передается с помощью шифрования, реализованных криптографическими методами. Такой комплекс мер образует трехступенчатую модель защиты информации.

4 МОДЕЛИ ЗАЩИТЫ ИНФОРМАЦИИ

После рассмотрения угроз информационной безопасности и методов защиты информации, становится возможно построить модель защиты информационной системы (с допустимым уровнем абстракции). Модели разделяются на общие, математические (отражает процессы в виде математической формулы) и графические (наглядно отражает процессы, происходящие в информационной системе).

Для определения качества функционирования систем защиты информации принято использовать формулу:

$$\overline{\mathrm{w}} = \sum_{i=1}^{n} (Pi_{\text{угр}} \cdot \Delta q_i^{\text{угр}} \cdot P_{i\text{угр}}^{\text{устр}}) \qquad (1)$$

где $\overline{W}$ - показатель качества функционирования системы защиты информации;

$P_{\text{i}}^{\text{угр}}$ - вероятность появления угрозы;

Δq_i $^{\text{угр}}$ - ущерб, приносимый информационной системе;

P_i $^{\text{угр устр}}$ - вероятность устранения каждой i - ой угрозы.

К недостаткам такой модели можно отнести невозможность определения вероятности преодоления нарушителем системы защиты информации. Другими словами, по общей математической модели невозможно оценить вероятность реализации несанкционированного доступа.

В качестве более усовершенствованной версии вышеописанной модели можно рассмотреть модель на рис.5.

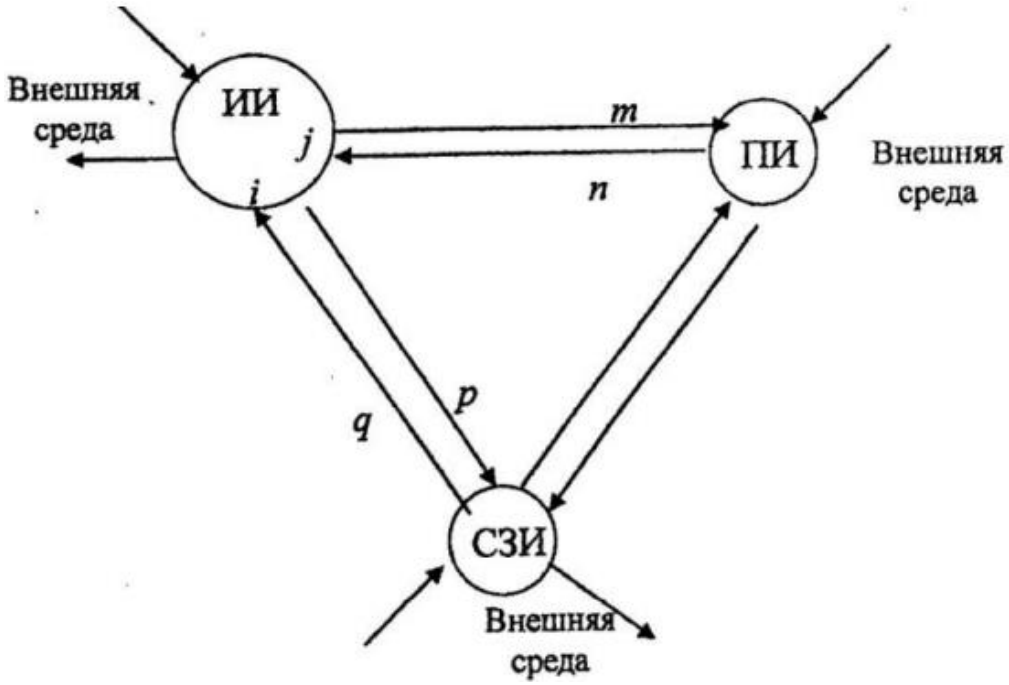

Рисунок 5. Общая модель защиты информации, с учетом влияния окружающей среды

В данной модели представлена взаимосвязь системы защиты информации (СЗИ) с источником информации(ИИ) и пользователем информации(ПИ). Причем, в отличие от предыдущей модели, учитывается влияние внешней среды на все компоненты информационной системы. Аналитическим выражением для этой модели выступает выражение:

$$\begin{cases} A_{0j} = A_j W_{ji} W_{0j} = (A_i W_{in} + A_q W_{iq} + A_{i0} W_{i0}) W_{ji} W_{0j} \\ A_{0q} = A_p W_{qp} W_{0p} = (A_i W_{ip} + A_n W_{pn} + A_{p9} W_{p0}) W_{qp} W_{0p} \\ A_{0n} = A_m W_{nm} W_{0n} = (A_j W_{mj} + A_q W_{mq} + A_{m0} W_{m0}) W_{nm} W_{0n} \end{cases} \quad (2)$$

Недостатком данной модели является её неспособность отражать процессы, происходящие внутри информационной системы. Это является серьезным минусом, так как именно внутренние процессы происходящие

внутри систем защиты информации важны для качественной оценки защиты информации.

К общим моделям защиты информации относится модель защиты с полным перекрытием угроз. В данной модели каждая угроза проходит через свой элемент системы защиты. Схему построения такой модели можно увидеть на рис.6.

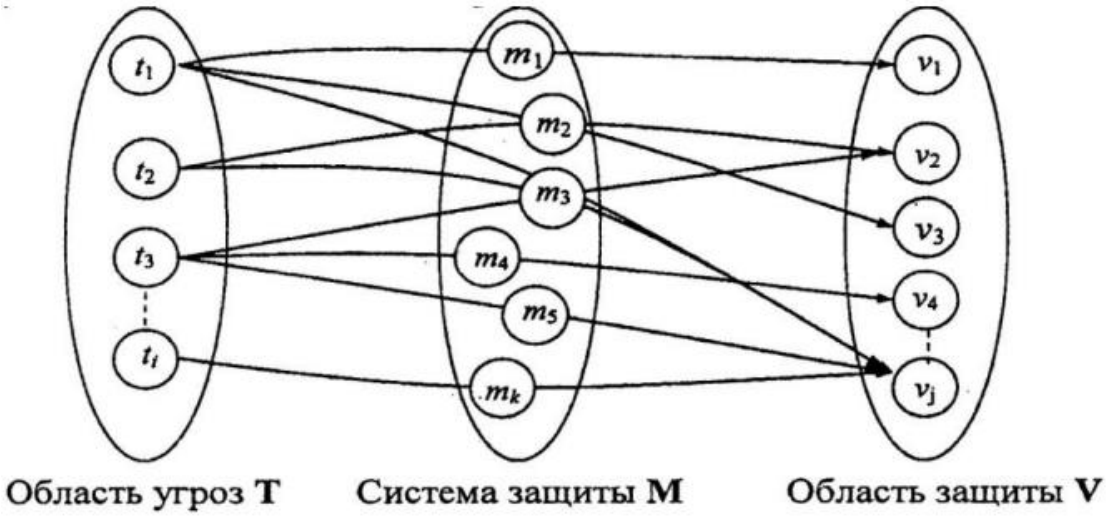

Рисунок 6. Модель защиты информации с полным перекрытием угроз

Все вышеперечисленные модели являются теоретической базой, необходимой на стадии проектирования систем безопасности, когда еще не сформирована структура системы, и необходимо дать предварительную оценку эффективности проектируемой системы.

В качестве моделей защиты информации с более низким уровнем абстракции выступают другие модели защиты. Рассмотрим самые известные из них.

Модель Биба –модель при который вводится разграничение субъектов и объектов на разные уровни доступа. Затем на их влияния накладываются два ограничения:

1. Субъект с более низким уровнем доступа не может получать информацию из объекта более высокого уровня.

2. Субъект с более высоким уровнем доступа не может изменять информацию в объекте более низкого доступа.

На рис.7 показана модель Бибы при двух уровнях доступа.

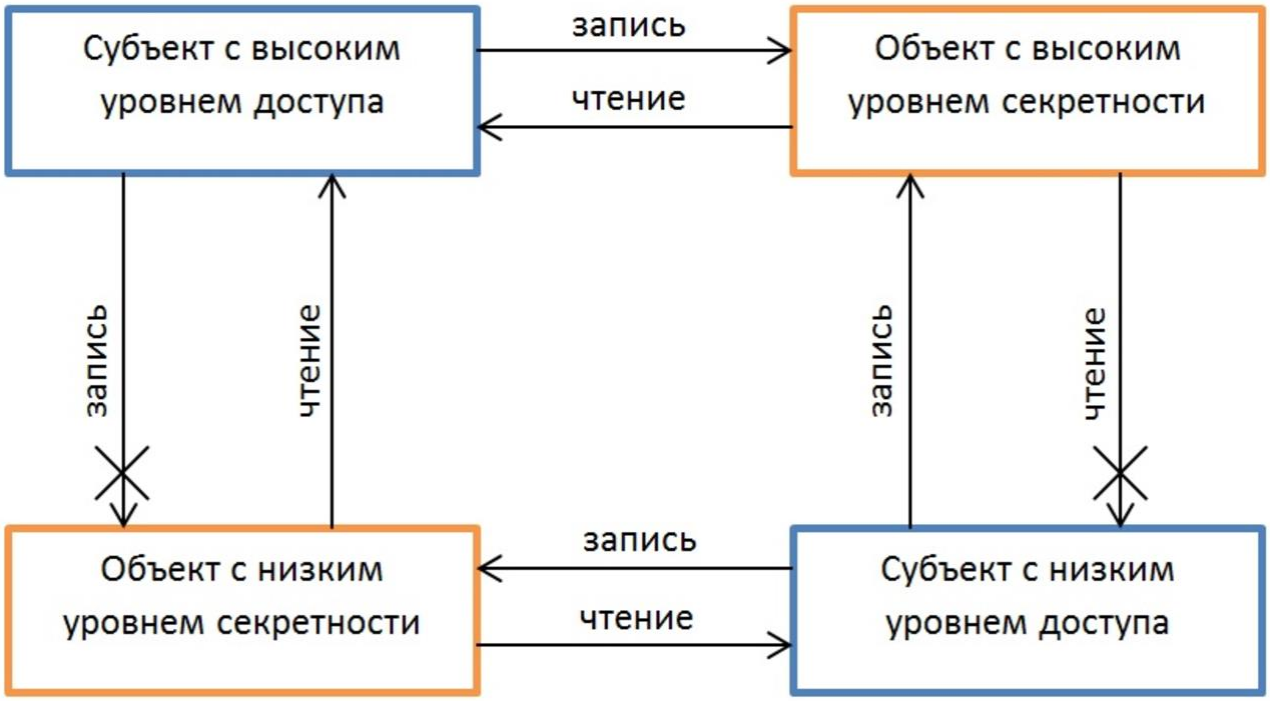

Рисунок 7. Модель Бибы при двух уровнях доступа

Другой моделью, используемой при создании систем защиты, является модель Деннинга. Данная модель подразумевает создание концентрированных колец защиты, где во внутренних кольцах хранится самая важная информация, а ближе к периферии – информация второстепенной важности. Соответственно, чем ближе к центру, тем более жестко организована безопасность информации, и чем дальше от центра, тем информация менее защищена. На рис.7 отображено схематическое представление модели Деннинга.

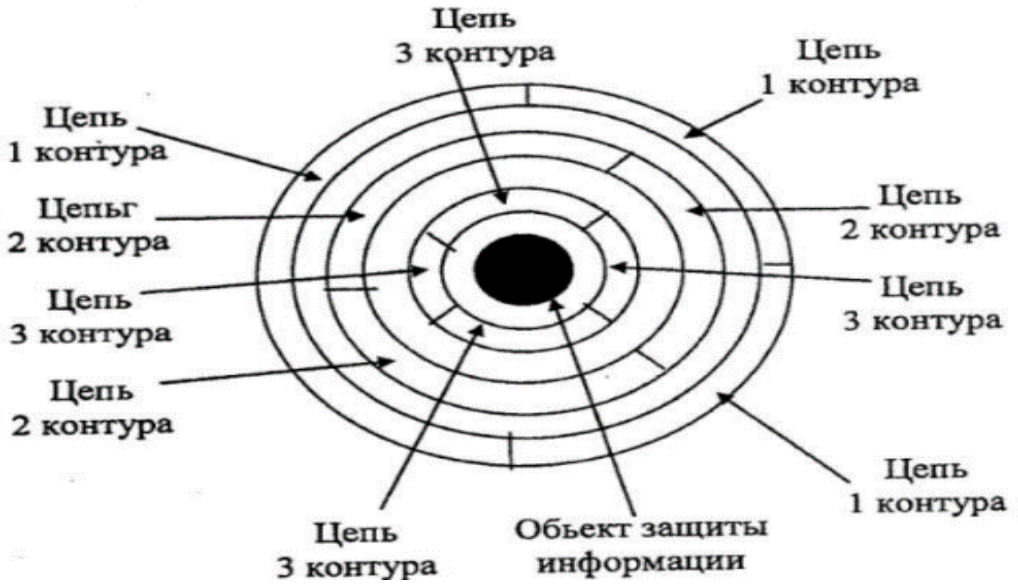

Рисунок 8. Модель Деннинга

В основу аналитического описания модели Деннинга легла оценка устойчивости препятствий многоуровневой защиты. В математическом виде модель Деннинга выглядит так:

$$P_{\text{сзи}} = 1 - \prod_{i=1}^{m}(1 - p_i) \qquad (3)$$

где $P_{\text{сзи}}$ –вероятность преодоления системы защиты информации,

i - порядковый номер преграды технической защиты информации,

i = 1,…,m; m- количество дублированных преград,

p_i - стойкость i-й преграды.

В свою очередь стойкость контура определяется:

$$P_{\text{блок}i} = \frac{t_H}{T_{\text{блок}}} \qquad (4)$$

$$p_i = P_{\text{блок}i}(1 - P_{\text{откл}}) \qquad (5)$$

$$P_{\text{откл}} = \exp(-\lambda t) \qquad (6)$$

Где $P_{\text{блок}i}$ – вероятность блокирования i - й преграды,

$P_{\text{отк}}$ – вероятность отказа системы защиты,

t_H – время преодоления преграды нарушителем,

$T_{\text{блок}}$ - время выявления и блокирования угрозы НСД,

λ - интенсивность отказа технических средств защиты,

t – время функционирования системы обнаружения и блокирования НСД.

Основой вышеперечисленных систем является использование диспетчера доступа, а сама система защиты предстает в виде тройки:

$$Z=<S,Q,P> \quad (7)$$

где S – пользователи и программы, а так же рожденные ими программы и процессы,

Q – множество объектов(ресурсов) системы, которые могут использоваться субъектами,

P – множество прав доступа субъектов к объектам.

Общий вид таких моделей представлен на рис.8.

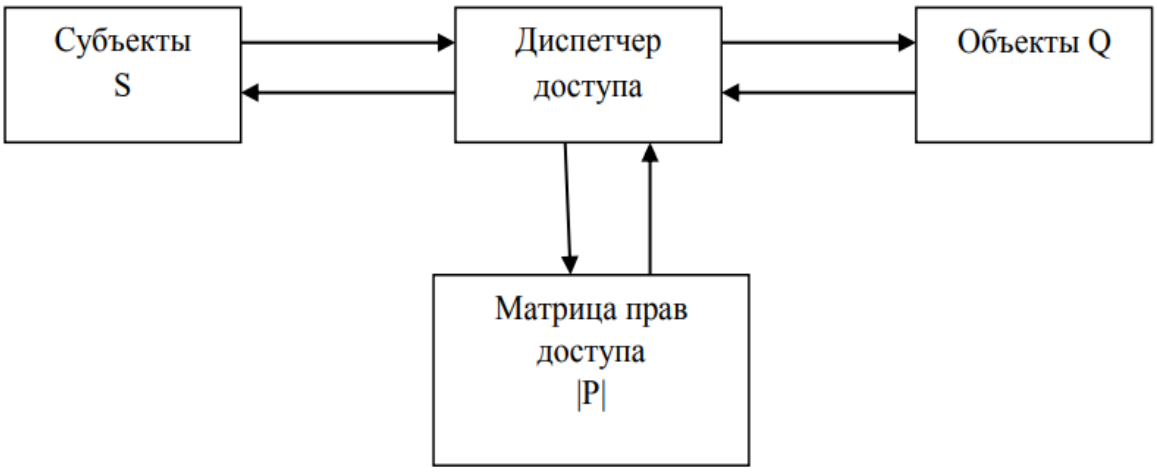

Рисунок 9. Общий вид моделей SQP

Кроме SQP-существует ряд других моделей, основанных на теории автоматов. Согласно данной теории, система всегда находится в одном из разрешенных состояний, и при любых действиях переходит между ними. Субъекты и объекты в таких моделях разбиваются на домены, после чего переход системы из одного состояния в другое происходит в соответствии с

таблицей разрешений. Так работает модель Гогена-Мизигера и Сазерлендская модель. Разница меду ними лишь в том, что в первой используются транзакции (подтверждения) при переходи из одного состояния в другое, а во второй исследуются все возможные композиции перехода.

Отдельного упоминания в системах защиты информации, основанных на теории автоматов, заслуживает модель Кларка-Вильсона. Эта модель основана на постоянном использовании транзакций и оформлении прав доступа субъектов к объектам. В данной модели впервые была рассмотрена защищенность третьей стороны. Под безопасностью третьей стороны подразумевается безопасность системы безопасности. Эту роль в системах безопасности начала играть программа супервизор. Так же в модели Кларка-Вильсона была введена новая система верификации субъектов. Верификация производилась не только перед выполнением команды от субъекта, но и повторно после ее выполнения. Это позволило решить проблему подмены субъекта в момент верификации.

5 СОЗДАНИЕ МОДЕЛИ ЗАЩИТЫ ИНФОРМАЦИИ

Создание модели системы защиты информации (СЗИ), является одним из этапов ввода СЗИ в работу. Для корректной работы, модель по которой СЗИ будет построена должна:

1. Соответствовать требованиям заказчика к СЗИ;
2. Отражать структуру субъектов и объектов информационной системы и их взаимодействия;
3. Стоимость реализации и эксплуатации СЗИ построенной по рассматриваемой модели, должна быть меньше, чем стоимость наиболее вероятного ущерба от реализации угроз.

Очевидно, что с таким объемом задач, не под силу справится одной модели. Поэтому при разработке СЗИ строят несколько моделей одной и той же системы, но отражающих различные аспекты её функционирования.

Основными двумя моделями, на которых основывается проектирование СЗИ, являются модель Данинга и модель Кларка-Вильсона. Первая модель отображает общий характер поведения объектов и субъектов в информационной системе, отображает уровни защиты, дает представление о времени, затратах на поддержание систем защиты, вероятности и ущербу от реализации угрозы. В свою очередь модель Кларка-Вильсона представляет систему, как автомат, с конечным числом состояний и дает представление о структуризации субъектов и объектов в информационной системе, о разделении прав доступа у субъектов к объектам и о возможном количестве состояний информационной системы, а также о способах перехода к этим состояниям.

На основе данных полученных из этих моделей уже можно выдвигать требования к правовой, технической и программной части реализации СЗИ. Однако, рекомендуется использовать и другие модели, для создания более четких требований и рассмотрению боле широкого спектра информационных угроз и методов защиты.

ЗАКЛЮЧЕНИЕ

В ходе выбора и выполнения практического задания, мной были получены знания о векторе развития Российской Федерации в области информационной безопасности, выделены и рассмотрены стандартные угрозы для информационных ресурсов предприятия, а также основные методы защиты.

На основе сопоставления угроз и методов защиты, были изучены разработанные модели для защиты информационных ресурсов, выявлены их сильные и слабые стороны, дано математическое и графическое представление каждой модели, рассмотрены примеры работы данных моделей.

Исходя из полученных в ходе анализа данных, была выполнена задача учебной практики, а именно, был разработан алгоритм создания универсальной модели защиты информационных ресурсов на предприятии и описан каждый шаг для его реализации.

СПИСОК ЛИТЕРАТУРЫ

1. «Аутентификация. Теория и практика обеспечения безопасного доступа к информационным ресурсам» Мир**,** 2020**.** - 552 с.
2. ГОСТ Р 50922-2006 «Защита информации. Основные термины и определения»
3. ГОСТ Р 53114-2008 «Защита информации. Обеспечение информационной безопасности в организации. Основные термины и определения.»
4. ГОСТ Р 56545-2015 «Защита информации. Уязвимости информационных систем. Правила описания уязвимостей.»
5. Доктрина Информационной Безопасности Российской Федерации (указ президента РФ от 5 декабря 2016 года № 646)
6. Баранова, Е.К. Информационная безопасность и защита информации / Е.К. Баранова. - М.: РИОР, 2018. - 165 с.
7. Васильков, А.В. Безопасность и управление доступом в информационных системах. Учебное пособие / А.В. Васильков. - М.: Форум, 2021**.** - 463 с.
8. Гришина, Н.В. Информационная безопасность предприятия / Н.В. Гришина. - М.: Форум, 2018. - 551 с.
9. Федеральный закон от 27.07.2006 N 149-ФЗ (ред. от 29.12.2022) "Об информации, информационных технологиях и о защите информации" (с изм. и доп., вступ. в силу с 01.03.2023)