**Анализ составленной модели угрозы безопасности.**

Основной угрозой являются внешние нарушители с низким потенциалом, а также средним потенциалом. К ним относятся бывшие работники (пользователи), конкурирующие организации, а также неустановленные внешние субъекты (физические лица).

Возможная мотивация вышепересиленных нарушителей следующая:

- Идеологические или политические мотивы.

-Причинение имущественного ущерба путем мошенничества или иным преступным путем.

-Любопытство или желание самореализации (подтверждение статуса).

-Выявление уязвимостей с целью их дальнейшей продажи и получения финансовой выгоды.

- Причинение имущественного ущерба путем мошенничества или иным преступным путем.

-Месть за ранее совершенные действия.

- Получение конкурентных преимуществ.

-Причинение имущественного ущерба путем обмана или злоупотребления доверием

Возможный класс СКЗИ: КС1. (для всех нарушителей)

**Уровень защищенности**

Уровень защищенности отображен в таблице, представленной ниже.

Таблица 1

|  |  |  |  |  |
| --- | --- | --- | --- | --- |
| **Структурно-функциональные характеристики информационной системы, условия ее эксплуатации** | | **Уровень проектной защищенности** | | |
| **Категория** | **Показатель** | **Высокий** | **Средний** | **Низкий** |
| По структуре информационной системы | Локальная информационная система | 0 | 1 | 0 |
| По используемым информационным технологиям | Системы на основе виртуализации | 0 | 0 | 1 |
| По используемым информационным технологиям | Системы, реализующие облачные вычисления | 0 | 0 | 1 |
| По используемым информационным технологиям | Системы с технологиями беспроводного доступа | 0 | 0 | 1 |
| По архитектуре информационной системы | Системы на основе тонкого клиента | 1 | 0 | 0 |
| По архитектуре информационной системы | Системы с удаленным доступом пользователей | 0 | 0 | 1 |
| По архитектуре информационной системы | Использование разных типов операционных систем | 0 | 1 | 0 |
| По наличию (отсутствию) взаимосвязей с иными информационными системами | Взаимодействующая с системами | 0 | 0 | 1 |
| По наличию (отсутствию) взаимосвязей (подключений) к сетям связи общего пользования | Подключенная | 0 | 0 | 1 |
| По размещению технических средств | Расположенные в пределах одной контролируемой зоны | 1 | 0 | 0 |
| По режимам обработки информации | Многопользовательский | 0 | 0 | 1 |
| По режимам разграничения прав доступа | С разграничением | 0 | 1 | 0 |
| По режимам разделения функций по управлению информационной системой | Выделение рабочих мест для администрирования в отдельный домен | 0 | 1 | 0 |
| По подходам к сегментированию информационной системы | Без сегментирования | 0 | 0 | 1 |
|  | Итог | 2 | 4 | 8 |
|  | % | 14.29% | 28.57% | 57.14% |

**Действия по повышению безопасности системы**

Действия по повышению безопасности системы можно предпринять нижеследующие.

Обеспечить:

* систему обеспечения информационной безопасности (под ней мы подразумеваем комплекс мероприятий (внутренние правила работы с данными, регламент передачи сведений, доступ к ним и т. д.) и технических средств (использование программ и приборов для сохранения конфиденциальности данных));
* разработку (создание новых), эксплуатацию и усовершенствование уже имеющихся средств защиты информации;
* перманентный контроль над действенностью принимаемых мер в области обеспечения информационной безопасности.

Последний пункт особенно важен. Без методики оценки очень трудно определить эффективность ИБ. Если эффективность падает, необходимо срочно вносить коррективы (для этого и нужна перманентность контроля).

Также можно ввести организационный метод обеспечения информационной безопасности, который имеет следующие составляющие:

* создание режима охраны информации;
* разработка правил взаимоотношений между сотрудниками;
* регламентация работы с документами;
* правила использования технических средств в рамках существующего правового поля РФ;
* аналитическая работа по оценке угроз информационной безопасности.