МИНОБРНАУКИ РОССИИ

Федеральное государственное бюджетное образовательное учреждение высшего образования

**«МИРЭА – Российский технологический университет»**

**РТУ МИРЭА**

Институт кибербезопасности и цифровых технологий

КБ-4 «Интеллектуальные системы информационной безопасности»

**Отчет** по практической работе №4 на тему: Расчет рисков по информационной системе

**по дисциплине:** «Управление информационной безопасностью»

**Выполнил:**
Студент группы ББМО-01-22
ФИО: Карев Д.П.

**Проверил:**

Р.В. Пимонов

**Москва 2023**

Содержание

## 1. Входные данные(ресурсы) для расчета рисков ИБ

В данной работе запланирован расчет рисков информационной безопасности для автоматизированной информационной системы ФГБУ «НПП «ГАММА»

Исходные данные возьмем из практический работ 1.3 “Создание политики информационной безопасности”, 1.6 “Построение модели нарушителя” и 1.8. “Построение модели угроз”.

Обратимся к работам, что взять оттуда исходные данные. Ресурсы взяты из пункта 2.1 практической работы 1.8. “Построение модели угроз” и показаны в таблице 1. Угрозы и возможные уязвимости также взяты из данной практической работы и также отражены в таблице 1.

Таблица 1 – Входные данные(ресурсы) для расчета рисков ИБ

| Источник | Угрозы | Уязвимости |
|---|---|---|
| **ЛВС (обмен информацией между сотрудниками компании)** | **Угроза 1** Атаки внутри сети и НСД | **Уязвимость 1** Отсутствие наблюдения(мониторинга) в компании. |
| | | **Уязвимость 2** Безалаберное отношение к техничке компании (отсутствие пароля на АРМ) |
| | **Угроза 2** Заражение систем вирусами, троянами, шпионскими программами | **Уязвимость 1** Отсутствие антивируса |
| | | **Уязвимость 2** Отсутствие обновления ПО |
| **Сервер с ИСПДн** | **Угроза 1** Dos атаки, атаки от внешнего сегмента | **Уязвимость 1** Недостаточная защита сервера, слабые пароли |
| | | **Уязвимость 2** Отсутствие средств защиты от DDoS-атак, недостаточная пропускная способность интернет-канала |

| | | |
|---|---|---|
| | **<u>Угроза 2</u>**<br>НСД к серверу, на котором хранятся БД ИСПДн | **Уязвимость 1**<br>Недостаточная защита сетевого трафика |
| | | **Уязвимость 2**<br>Отсутствие двухфакторной аутентификации |
| | | **Уязвимость 3**<br>Использование несертифицированных средств защиты информации |
| | **<u>Угроза 3</u>**<br>Старое ПО | **Уязвимость 1**<br>Отсутствие регламентированных настроек сети |
| | | **Уязвимость 2**<br>Отсутствие обновления средств информационной безопасности |
| **ИСПДн ФГБУ «НПП «ГАММА»** | **<u>Угроза 1</u>**<br>НСД к ресурсам ИСПДн | **Уязвимость 1**<br>Малая защита средств связи и АРМ |
| | | **Уязвимость 2**<br>Неправильная настройка и управление правами доступа пользователей и администраторов |
| | **<u>Угроза 2</u>**<br>Утечка конфиденциальной информации, нарушение конфиденциальности клиентов | **Уязвимость 1**<br>Уволенные сотрудники |
| | | **Уязвимость 2**<br>Недостаточное шифрование данных |

Отобразим вероятности реализации угрозы через уязвимость в течение года и критичности реализации угрозы через данную уязвимость для каждого объекта ИСПДН ФГБУ «НПП «ГАММА». Входные данные для расчёта рисков информационной безопасности для источников представлены в таблице 2.

Таблица 2 – Входные данные для расчёта рисков информационной безопасности для источников ФГБУ «НПП «ГАММА»

| **Источник 1: ЛВС** | | |
|---|---|---|
| **Угроза/уязвимость** | **Вероятность реализации угрозы через уязвимость в течении года %, P(V)** | **Критичность реализации угрозы через данную уязвимость %, ER** |
| Угроза 1 /Уязвимость 1 | 50 | 60 |
| Угроза 1 /Уязвимость 2 | 20 | 60 |
| Угроза 2 /Уязвимость 1 | 60 | 40 |
| Угроза 2 /Уязвимость 2 | 10 | 40 |
| **Источник 2: Сервер с ИСПДн** | | |
| Угроза 1 /Уязвимость 1 | 50 | 80 |
| Угроза 1 /Уязвимость 2 | 60 | 80 |
| Угроза 2 /Уязвимость 1 | 70 | 70 |
| Угроза 2 /Уязвимость 2 | 90 | 70 |
| Угроза 3 /Уязвимость 1 | 40 | 50 |
| Угроза 3 /Уязвимость 1 | 75 | 50 |
| **Источник 3: ИСПДн** | | |
| Угроза 1 /Уязвимость 1 | 70 | 70 |
| Угроза 1 /Уязвимость 2 | 90 | 70 |
| Угроза 2 /Уязвимость 1 | 60 | 80 |
| Угроза 2 /Уязвимость 2 | 50 | 80 |

Отобразим результаты расчета уровня угрозы по уязвимости по формуле, через которую она может быть реализована в таблице 3.

Таблица 3 – Итоги расчёта показателей Th, CTh для источников ФГБУ «НПП «ГАММА»

| **Угроза/уязвимость** | **Уровень угрозы по каждой уязвимости %, Th** $\mathrm{Th} = \frac{ER}{100} \times \frac{P(V)}{100}$ | **Уровень угрозы по всем уязвимостям, через которые она может быть реализована %, CTh** $\mathrm{CTh} = 1 - \prod_{i=1}^{n}(1 - Th)$ |
|---|---|---|
| **Источник 1: ЛВС** | | |
| Угроза 1 /Уязвимость 1 | 0,3 | 0,384 |
| Угроза 1 /Уязвимость 2 | 0,12 | |
| Угроза 2 /Уязвимость 1 | 0,24 | 0.27 |
| Угроза 2 /Уязвимость 2 | 0,04 | |
| **Источник 2: Сервер с ИСПДн** | | |
| Угроза 1 /Уязвимость 1 | 0,4 | 0,754 |
| Угроза 1 /Уязвимость 2 | 0,48 | |
| Угроза 2 /Уязвимость 1 | 0,49 | 0,8113 |
| Угроза 2 /Уязвимость 2 | 0,69 | |
| Угроза 3 /Уязвимость 1 | 0,2 | 0,5 |
| Угроза 3 /Уязвимость 2 | 0,375 | |
| **Источник 3: ИСПДн** | | |
| Угроза 1 /Уязвимость 1 | 0,48 | 0,688 |
| Угроза 1 /Уязвимость 2 | 0,64 | |
| Угроза 2 /Уязвимость 1 | 0,05 | 0,079 |
| Угроза 2 /Уязвимость 2 | 0,07 | |

После расчета уровней угрозы по каждой уязвимости (Th) и по всем уязвимостям (CTh) для каждого ресурса ИС произведем расчет общего уровня угроз (CThR), действующего на источники и Расчет итогового риска по ресурсу (R) для каждого источников ФГБУ «НПП «ГАММА»

Таблица 4 – Итоги расчёта показателя CThR для источников ФГБУ «НПП «ГАММА»

| **Угроза/уязвимость** | **Уровень угрозы по всем уязвимостям, через которые она может быть реализована %, CTh** $CTh = 1 - \prod_{i=1}^{n}(1 - Th)$ | **Общий уровень угроз по ресурсу %, CThR** $CThR = 1 - \prod_{i=1}^{n}(1 - CTh_i)$ |
|---|---|---|
| **Источник 1: ЛВС** | | |
| Угроза 1 /Уязвимость 1 | 0,384 | 0,896 |
| Угроза 1 /Уязвимость 2 | | |
| Угроза 2 /Уязвимость 1 | 0,27 | |
| Угроза 2 /Уязвимость 2 | | |
| **Источник 2: Сервер с ИСПДн** | | |
| Угроза 1 /Уязвимость 1 | 0,688 | 0,9705 |
| Угроза 1 /Уязвимость 2 | | |
| Угроза 2 /Уязвимость 1 | 0,8113 | |
| Угроза 2 /Уязвимость 2 | | |
| Угроза 3 /Уязвимость 1 | 0,5 | |
| Угроза 3 /Уязвимость 2 | | |
| **Источник 3: ИСПДн** | | |
| Угроза 1 /Уязвимость 1 | 0,688 | 0,946 |
| Угроза 1 /Уязвимость 2 | | |
| Угроза 2 /Уязвимость 1 | 0,079 | |
| Угроза 2 /Уязвимость 2 | | |

После расчета уровней угрозы по каждой уязвимости (CThR) произведем риск по ресурсам.

Таблица 5 – Итоги расчёта показателя (**CR)** для источников ФГБУ «НПП «ГАММА»

| **Источник** | **Общий уровень угроз по ресурсу %, CThR** $CThR = 1 - \prod_{i=1}^{n}(1 - CTh_i)$ | **Риск по ресурсу у.е., R** |
|---|---|---|
| ЛВС | 0,896 | 89,6 |
| Сервер с ИСПДн | 0,9705 | 97,05 |
| ИСПДн | 0,946 | 94,6 |

Таким образом, в результате расчётов риск по ресурсам **(CR) равен 281,25 условных единиц.**

## 2. Рекомендации по улучшению мер защиты объекта ИСПДн

1. Регулярно проверять систему на безопасность.
2. Ограничивать права доступа, придерживаться принципа наименьших привилегий.
3. Реализовать строгого управления доступом с использованием принципов наименьших привилегий.
4. Регулярное обновлять программного обеспечения и операционных систем с применением последних патчей безопасности для устранения известных уязвимостей.
5. Установить системы мониторинга для раннего обнаружения угроз.
6. Проводить регулярные тренинги по безопасности.
7. Регулярно обновлять программное обеспечение и устанавливать патчи безопасности.