Изображение выглядит как корона

Автоматически созданное описание

МИНОБРНАУКИ РОССИИ

Федеральное государственное бюджетное образовательное учреждение

высшего образования

**«МИРЭА – Российский технологический университет»**

**РТУ МИРЭА**

ИКБ направление «Киберразведка и противодействие угрозам с применением технологий искусственного интеллекта» 10.04.01

Кафедра КБ-4 «Интеллектуальные системы информационной безопасности»

**Расчет рисков информационной безопасности**

по дисциплине

«Управление информационной безопасностью»

Группа:

ББМО-01-22

Выполнил:

Феденёв А.В.

Проверил:

Пимонов Р.В.

Москва 2023

В практической работе рассмотрим расчет рисков только для одного ресурса ИС.

|  |  |
| --- | --- |
| **Угрозы** | **Уязвимости** |
| НСД к ресурсам ИСПДн | Оставление устройств разблокированными, недостаточная защита компьютеров и мобильных устройств |
| Неправильная настройка и управление правами доступа пользователей и администраторов |
| Утечка конфиденциальной информации, нарушение конфиденциальности клиентов | Уволенные сотрудники |
| Недостаточное шифрование данных |
| Отсутствие строгих политик и процедур удаленной работы | Использование незащищенных или устаревших протоколов связи при удаленном доступе |
| Подключение к общедоступным Wi-Fi сетям без использования защищенных виртуальных частных сетей (VPN) |
| Сбой в сетевой инфраструктуре | Неэффективные меры предотвращения и защиты от распределенных атак на отказ в обслуживании (DDoS) |
| Отсутствие регулярных обновлений и патчей для сетевых устройств |
| Отсутствие строгих процессов управления учетными записями | Неэффективное журналирование и мониторинг действий пользователей |
| Неиспользование автоматизированных средств для эффективного управления жизненным циклом учетных записей |

Отобразим вероятности реализации угрозы через уязвимость в течение года и критичности реализации угрозы через данную уязвимость.

|  |  |  |
| --- | --- | --- |
| **Угроза/уязвимость** | **Вероятность реализации угрозы через данную уязвимость в течение года, %, P(V)** | **Критичность реализации угрозы через данную уязвимость, %, ER** |
| Угроза 1/ уязвимость 1 | 30 | 40 |
| Угроза 1/ уязвимость 2 | 70 | 75 |
| Угроза 2/ уязвимость 1 | 25 | 35 |
| Угроза 2/ уязвимость 2 | 30 | 55 |
| Угроза 3/ уязвимость 1 | 50 | 65 |
| Угроза 3/ уязвимость 2 | 30 | 55 |
| Угроза 4/ уязвимость 1 | 25 | 50 |
| Угроза 4/ уязвимость 2 | 30 | 55 |
| Угроза 5/ уязвимость 1 | 15 | 20 |
| Угроза 5/ уязвимость 2 | 30 | 40 |

Отобразим результаты расчёта уровня угрозы по каждой уязвимости, уровня угрозы по всем уязвимостям, через которые она может быть реализована, общего уровня угроз по ресурсу и риска по ресурсу.

|  |  |  |  |  |
| --- | --- | --- | --- | --- |
| **Угроза/уязвимость** | **Уровень угрозы по каждой уязвимости %, Th** | **Уровень угрозы по всем уязвимостям, через которые она может быть реализована %, CTh** | **Общий уровень угроз по ресурсу %, CThR** | **Риск по ресурсу, у.е** |
| Угроза 1/ уязвимость 1 | 0,12 | 0,586 | 0,8928 | 89,28 |
| Угроза 1/ уязвимость 2 | 0,53 |
| Угроза 2/ уязвимость 1 | 0,09 | 0,245 |
| Угроза 2/ уязвимость 2 | 0,17 |
| Угроза 3/ уязвимость 1 | 0,33 | 0,444 |
| Угроза 3/ уязвимость 2 | 0,17 |
| Угроза 4/ уязвимость 1 | 0,13 | 0,278 |
| Угроза 4/ уязвимость 2 | 0,17 |
| Угроза 5/ уязвимость 1 | 0,03 | 0,146 |
| Угроза 5/ уязвимость 2 | 0,12 |

В результате риск по ресурсам получился 89.

**Рекомендации по снижению уровня риска информационной безопасности:**

* Проводить регулярные аудиты безопасности для выявления и устранения потенциальных слабых мест в системе, а также для проверки соответствия стандартам безопасности;
* Ограничение доступа к важным данным. Установление ролевой модели;
* Введение контроля за носителями и источниками информации;
* Организация шифрования данных;
* Внедрение актуальных технических решений для контроля и мониторинга информационных ресурсов организации;
* Регулярно создавать резервные копии данных и разработать план восстановления после инцидента (DRP) для минимизации потерь данных и снижения времени восстановления в случае инцидента.