

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»

Практическая работа № 4

**Расчёт рисков информационной безопасности на основе исходных данных ФГБУ «Редакция «Российской газеты»**

по дисциплине

«Управление информационной безопасностью»

Группа:

ББМО-02-22

Выполнил:

Агишевский П. Д.

Проверил:

Пимонов Р. В.

Москва, 2024

Содержание

[1. Обозначения и сокращения 4](#_Toc157018417)

[2. Введение 5](#_Toc157018418)

[3. Вводные данные 5](#_Toc157018419)

[4. Расчёт рисков 7](#_Toc157018420)

[5. Рекомендации по снижению уровня риска ИБ 8](#_Toc157018421)

[6. Повторный расчёт рисков 8](#_Toc157018422)

# Обозначения и сокращения

|  |  |  |
| --- | --- | --- |
| ИС | – | Информационная система |
| БД | – | База данных |
| ИСПДн | – | Информационная система персональных данных |
| ЛВС | – | Локальная вычислительная сеть |
| НСД | – | Несанкционированный доступ |
| ОС | – | Операционная система |
| ПДн | – | Персональные данные |
| ПО | – | Программное обеспечение |
| ЦОД | – | Центр обработки данных |
| АРМ | – | Автоматизированное рабочее место |
| ИБ | – | Информационная безопасность |
|  |  |  |
|  |  |  |
|  |  |  |
|  |  |  |
|  |  |  |

# Введение

В данной практической работе будет произведён расчет рисков системы, описываемой в практических работах 1-3. Для этого необходимо установить следующие:

Ресурсами для расчета рисков – было решено взять объекты воздействия из разработанной ранее модели угроз.

# Вводные данные

В качестве угроз – будут выступать сгруппированные угрозы из БДУ ФСТЭК России, например, угрозы НСД, повышения привилегий, отказ в обслуживании и т.д.

В качестве уязвимостей – будут выбраны недостатки инфраструктуры, наличие которых так или иначе допускает реализацию угроз.

Перечень угроз и уязвимостей по одному ресурсу ИС представлен в таблице 1.

Таблица 1 – Угрозы и уязвимости ФГБУ «Редакция «Российской газеты»

|  |  |  |
| --- | --- | --- |
| **Ресурс** | **Угрозы** | **Уязвимости** |
| Информационные сисемы ФГБУ «Редакция «Российской газеты» | 1. НСД к ресурсам ИСПДн | 1. Оставление устройств разблокированными, недостаточная защита компьютеров и мобильных устройств |
| 1. Неправильная настройка и управление правами доступа пользователей и администраторов |
| 1. Уязвимость программного и программно-аппаратного обеспечения |
| 1. Утечка конфиденциальной информации, нарушение конфиденциальности клиентов | 1. Уволенные сотрудники |
| 1. Недостаточное шифрование данных |
| 1. Нечёткие формулировки в регламенте о разглашении информации |
| 1. Отсутствие строгих политик и процедур удаленной работы | 1. Использование незащищенных или устаревших протоколов связи при удаленном доступе |
| 1. Подключение к общедоступным Wi-Fi сетям без использования защищенных виртуальных частных сетей (VPN) |
| 1. Сбой в сетевой инфраструктуре | 1. Неэффективные меры предотвращения и защиты от распределенных атак на отказ в обслуживании (DDoS) |
| 1. Отсутствие регулярных обновлений и патчей для сетевых устройств |
| 1. Старое ПО, отсутствие обновления средств информационной безопасности |
| 1. Отсутствие строгих процессов управления учетными записями | 1. Неэффективное журналирование и мониторинг действий пользователей |
| 1. Неиспользование автоматизированных средств для эффективного управления жизненным циклом учетных записей |

Далее будут отображены вероятности реализации угроз через уязвимости в течение года и критичности реализации угроз через конкретные уязвимости для информационных систем ФГБУ «Редакция «Российской газеты» в таблице 2.

Таблица 2 – Входные данные для расчёта рисков информационной безопасности для ИС ФГБУ «Редакция «Российской газеты»

|  |  |  |
| --- | --- | --- |
| **Угроза/уязвимость** | **Вероятность реализации угрозы через данную уязвимость в течение года, %, P(V)** | **Критичность реализации угрозы через данную уязвимость, %, ER** |
| Угроза 1/ уязвимость 1 | 40 | 75 |
| Угроза 1/ уязвимость 2 | 70 | 50 |
| Угроза 1/ уязвимость 3 | 25 | 70 |
| Угроза 2/ уязвимость 1 | 30 | 30 |
| Угроза 2/ уязвимость 2 | 20 | 50 |
| Угроза 2/ уязвимость 3 | 40 | 60 |
| Угроза 3/ уязвимость 1 | 50 | 60 |
| Угроза 3/ уязвимость 2 | 30 | 55 |
| Угроза 4/ уязвимость 1 | 40 | 55 |
| Угроза 4/ уязвимость 2 | 30 | 55 |
| Угроза 4/ уязвимость 3 | 35 | 50 |
| Угроза 5/ уязвимость 1 | 20 | 25 |
| Угроза 5/ уязвимость 2 | 25 | 30 |

# Расчёт рисков

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 для ФГБУ «Редакция «Российской газеты»в таблице 3. Критичность ресурса (D) для “Информационные системы Организации” равна 70%. Уровень принятия риска менее 50%.

Таблица 3 – Расчёт рисков ИБ для ФГБУ «Редакция «Российской газеты»

|  |  |  |  |
| --- | --- | --- | --- |
| **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** |
| Угроза 1/ уязвимость 1 | 30 | 62 | 65 |
| Угроза 1/ уязвимость 2 | 35 |
| Угроза 1/ уязвимость 3 | 18 |
| Угроза 2/ уязвимость 1 | 9 | 38 |
| Угроза 2/ уязвимость 2 | 10 |
| Угроза 2/ уязвимость 3 | 24 |
| Угроза 3/ уязвимость 1 | 30 | 42 |
| Угроза 3/ уязвимость 2 | 17 |
| Угроза 4/ уязвимость 1 | 22 | 46 |
| Угроза 4/ уязвимость 2 | 17 |
| Угроза 4/ уязвимость 3 | 18 |
| Угроза 5/ уязвимость 1 | 5 | 12 |
| Угроза 5/ уязвимость 2 | 8 |

# Рекомендации по снижению уровня риска ИБ

* Проводить регулярные аудиты безопасности для выявления и устранения потенциальных слабых мест в системе, а также для проверки соответствия стандартам безопасности;
* Внести правки в регламент о разглашении информации, чтобы изложенная там информация была понятна читателю.
* 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;
* Реализовать механизмы защиты от Dos/DDoS атак.
* Регулярно создавать резервные копии данных и разработать план восстановления после инцидента (DRP) для минимизации потерь данных и снижения времени восстановления в случае инцидента.

# Повторный расчёт рисков

После применения рекомендаций перерасчитаем риски. 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 ФГБУ «Редакция «Российской газеты» в таблице 4. Критичность ресурса (D) для “Информационные системы Организации” равна 70%.

Таблица 4 – Повторный расчёт рисков ИБ для ФГБУ «Редакция «Российской газеты»

|  |  |  |  |  |  |
| --- | --- | --- | --- | --- | --- |
| **Угроза/уязвимость** | **Вероятность реализации угрозы через уязвимость в течении года %, P(V)** | **Критичность реализации угрозы через данную уязвимость %, ER** | **Уровень угрозы по каждой уязвимости %, Th** | **Уровень угрозы по всем уязвимостям, через которые она может быть реализована %, CTh** | **Общий уровень угроз по ресурсу %, CThR** |
| Угроза 1/ уязвимость 1 | 15 | 75 | 11 | 32 | 48 |
| Угроза 1/ уязвимость 2 | 35 | 50 | 18 |
| Угроза 1/ уязвимость 3 | 10 | 70 | 7 |
| Угроза 2/ уязвимость 1 | 15 | 30 | 5 | 18 |
| Угроза 2/ уязвимость 2 | 5 | 50 | 3 |
| Угроза 2/ уязвимость 3 | 20 | 60 | 12 |
| Угроза 3/ уязвимость 1 | 25 | 60 | 15 | 24 |
| Угроза 3/ уязвимость 2 | 20 | 55 | 11 |
| Угроза 4/ уязвимость 1 | 20 | 55 | 11 | 22 |
| Угроза 4/ уязвимость 2 | 10 | 55 | 6 |
| Угроза 4/ уязвимость 3 | 15 | 50 | 8 |
| Угроза 5/ уязвимость 1 | 5 | 25 | 1 | 6 |
| Угроза 5/ уязвимость 2 | 15 | 30 | 5 |

После применения рекомендаций риск снизился с 65% до 48% и теперь соответствует уровню принятия риска менее 50%.