

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**

по дисциплине: «Управление информационной безопасностью»   
На тему:

«Расчет рисков информационной безопасности»

Группа:

ББМО-01-22

Выполнил:

Гребенник Г.С

Проверил:

Пимонов Р.В.

Москва, 2023

**СОДЕРЖАНИЕ**

[ВВЕДЕНИЕ 3](#_Toc156848389)

[**1 Входные данные (ресурсы) для расчета рисков ИБ** 3](#_Toc156848390)

[**2 Расчет рисков ИБ на основе модели нарушителя и модели угроз** 4](#_Toc156848391)

[3 Рекомендации по улучшению мер защиты объекта ИСПДн 4](#_Toc156848392)

[**ЗАКЛЮЧЕНИЕ** 6](#_Toc156848393)

# ВВЕДЕНИЕ

В данной практической работе, нам необходимо произвести расчет рисков системы, описываемой в практических работах 1-3.Для оценки рисков информационной системы организации защищенность каждого ценного ресурса определяется при помощи анализа угроз, действующих на конкретный ресурс, и уязвимостей, через которые данные угрозы могут быть реализованы. Оценивая вероятность реализации актуальных для ценного ресурса угроз и степень влияния реализации угрозы на ресурсы, анализируются информационные риски ресурсов организации.

**1 Входные данные (ресурсы) для расчета рисков ИБ**

Оценивая вероятность реализации актуальных для ценного ресурса угроз и степень влияния реализации угрозы на ресурсы, анализируются информационные риски ресурсов организации.

В данной практической работе будет произведен расчет рисков информационной безопасности для ИСПДн АО «Россети» (далее «Россети»). Защищенность каждого ценного ресурса определяется при помощи анализа угроз, действующих на конкретный ресурс, и уязвимостей, через которые данные угрозы могут быть реализованы. Исходными данными для выполнения практического задания являются данные, полученные из предыдущих работ. Они приведены в таблице 1.

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

|  |  |  |
| --- | --- | --- |
| **Объект (Ресурс)** | **Угрозы** | **Уязвимости** |
| 1. ИС персональных данных сотрудников, поставщиков и заказчиков АО «Россети» | 1.1 Разглашение  конфиденциальных данных | 1.1.1 Неправильный контроль доступа к данным организации |
| 1.2 Подмена данных, содержащих платежную информацию, информацию о проектах. Хищение денежных средств со счета организации | 1.2.1 Неправильный контроль доступа к данным организации, а также недостаточная организация защиты административных учетных записей |
| 2. ПО организации «Россети» | 2.1 Атака вредоносным ПО | 2.1.1 Отсутствие регламента работы с ПО |
| 2.1.2 Устаревшее ПО, отсутствие наличия обновлений |
| 3. Сервер, на котором хранится БД ИСПДн организации | 3.1 Отсутствие необходимых актуальных мер по обеспечению безопасности данных | 3.1.1 Отсутствие актуальных механизмов управления доступом и контроля привилегий |
| 3.1.2 Отсутствие методов шифрования данных |

**2 Расчет рисков ИБ на основе модели нарушителя и модели угроз**

Укажем вероятности реализации угроз через уязвимости для каждого ресурса ИС Россети (табл. 2).

Таблица 2 – Вероятности реализации угроз

|  |  |  |
| --- | --- | --- |
| **Угроза/уязвимость** | **Вероятность реализации угрозы через уязвимость в течении года %, P(V)** | **Критичность реализации угрозы через данную уязвимость %, ER** |
| 1. ИС персональных данных сотрудников, поставщиков и заказчиков ООО «Россети» | | |
| 1.1/1.1.1 | 35 | 40 |
| 1.2/1.2.1 | 15 | 40 |
| 2. ПО организации «Россети» | | |
| 2.1/2.1.1 | 55 | 50 |
| 2.1/2.1.2 | 60 | 40 |
| 3. Сервер, на котором хранится БД ИСПДн организации | | |
| 3.1/3.1.1 | 40 | 45 |
| 3.1/3.1.2 | 50 | 65 |

Теперь произведем расчет уровней угроз через уязвимости (Th) и по всем уязвимостям (CTh) для каждого ресурса ИС по определённым формулам. Также произведем расчет общего уровня угроз (CThR), действующего на объект и расчет итогового риска по ресурсу (R) для каждого объекта ИСПДн «Россети». Расчетные значения для каждого объекта ИСПДн «Россети» представлены в таблице 3.

Таблица 3 – Расчетные значения по всем показателям

|  |  |  |  |  |
| --- | --- | --- | --- | --- |
| **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., R** |
| 1. ИС персональных данных сотрудников, поставщиков и заказчиков АО «Россети» | | | | |
| 1.1/1.1.1 | 0,14 | 0,14 | 0,136 | 13,6 |
| 1.2/1.2.1 | 0,06 | 0,06 |
| 2. ПО организации «Россети» | | | | |
| 2.1/2.1.1 | 0,275 | 0,4351 | 0,4351 | 43,51 |
| 2.1/2.1.2 | 0,24 |
| 3. Сервер, на котором хранится БД ИСПДн организации | | | | |
| 3.1/3.1.1 | 0,18 | 0,4465 | 0,4465 | 44,65 |
| 3.1/3.1.2 | 0,325 |

Итог: (CR) равен 101,76 условных единиц.

# 3 Рекомендации по улучшению мер защиты объекта ИСПДн

1. Необходимо внедрение современных средств защиты информации, таких как межсетевые экраны, антивирусное программное обеспечение и системы обнаружения вторжений.
2. Внедрить двухфакторную аутентификацию.
3. Следует проводить регулярные обучающие семинары для сотрудников с целью повышения их осведомленности правил работы с конфиденциальной информацией, а также знать основы ИБ.
4. Разработать и внедрить политики и процедуры, которые будут регулировать работу с персональными данными и обеспечивать их защиту.
5. Регулярно обновлять систему и антивирусное ПО.
6. Следует регулярно проводить мониторинг и аудит информационной системы на предмет уязвимостей и возможных угроз ИС.
7. Рекомендуется внедрить систему обнаружения и предотвращения утечек данных (DLP), которая поможет предотвратить несанкционированный доступ к конфиденциальной информации.
8. Ввести контроль за носителями и источниками информации.
9. Создание системы резервного копирования данных и регулярного тестирования процедур восстановления информации в случае возникновения инцидентов.
10. Необходимо реализовать политику паролей для учетных записей удаленного доступа на основе передовых методик.
11. Необходимо будет развернуть сеть VPN, чтобы обеспечить подключение пользователей с удаленным доступом на основе технологий IP-безопасности (IPSec), SSL (Secure Sockets Layer) и SSH (Secure Shell).

**ЗАКЛЮЧЕНИЕ**

В ходе выполнения практической работы был проведен расчет рисков ИСПДн АО «Россети». В результате расчета параметра – риск ресурса информационной системы, мы можем получить численное представление такого критерия как риск. Опираясь на пороговое значения, аналитику и руководству предприятия проще контролировать результативность внедрения мер защиты и потенциальные убытки в результате инцидента на ресурс ИС.