

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 №2**

по дисциплине: «Управление информационной безопасностью»   
На тему:

«Разработка модели нарушителя»

Группа:

ББМО-01-22

Выполнил:

Гребенник Г.С

Проверил:

Пимонов Р.В.

Москва, 2023

Акционерное общество «Россети»

**Политика информационной безопасности**

АО «Россети»

г. Москва

2023 г.

**СОДЕРЖАНИЕ**

[**Введение** 4](#_Toc156846024)

[**1 Определение возможных объектов воздействия угроз безопасности информации в АО «Россети»** 4](#_Toc156846025)

# **Введение**

В данной практической работе будет проведена оценка угроз безопасности информации АО «Россети» целью которой является выявление подверженных несанкционированному доступу или воздействию сетей, информационных ресурсов и компонентов систем, которые могут привести к отрицательным последствиям. Работа направлен на выделение объектов воздействия и идентификацию источников угроз безопасности, с последующей формулировкой модели потенциального нарушителя. В данном контексте источник угрозы безопасности информации представляет собой субъект, будь то физическое лицо, материальный объект или физическое явление, являющийся непосредственной причиной возникновения угрозы.

# **1 Определение возможных объектов воздействия угроз безопасности информации в АО «Россети»**

Для начала определим виды ущерба в таблице 1.1

Таблица 1.1 виды ущерба и возможные негативные последствия

| **Идентификатор** | **Виды риска (ущерба)** | **Идентификатор** | **Возможные негативные последствия** |
| --- | --- | --- | --- |
| У1 | Ущерб физическому лицу | НП1 | Нарушение конфиденциальности (утечка) персональных данных. |
| НП2 | Разглашение  персональных данных. |
| У2 | Риски юридическому лицу, индивидуальному предпринимателю, связанные с хозяйственной деятельностью | НП3 | Необходимость дополнительных (незапланированных) затрат на закупку товаров, работ или услуг (в том числе закупка программного обеспечения, технических средств, вышедших из строя, замена, настройка, ремонт указанных средств). |
| НП4 | Нарушение штатного режима функционирования автоматизированной системы управления и управляемого объекта и/или процесса. |
| НП5 | Невозможность решения задач (реализации функций) или снижение эффективности решения задач (реализации функций). |

Определения объектов воздействия и видов воздействия на них представлены в таблице 1.2.

Таблица 1.2 – Возможные объекты воздействия угроз безопасности информации

|  |  |  |
| --- | --- | --- |
| **Негативные последствия** | **Объекты воздействия** | **Виды воздействия** |
| Потеря, изменение или хищение данных | Сервер, база данных информационной системы, содержащая конфиденциальную информацию | Подмена данных, содержащихся на сервере. |
| АРМ сотрудников организации | - Подмена данных, содержащих платёжную информацию, информацию о проектах  - Отправка фишинговых писем с недостоверной информацией или доступ к системе, с последующими заказами материалов |
| Нарушение работоспособности программно-аппаратных средств обработки, передачи и хранения информации | Программно-аппаратные средства обработки и хранения информации | Несанкционированный доступ к составляющим с последующим хищением жёсткого диска, либо добавление своего USB-носителя |
| Хищение денежных средств со счета организации (У2) | Банк-клиент | Несанкционированная подмена данных, содержащихся в реквизитах платежного поручения |
| АРМ главного бухгалтера | Подмена данных, содержащих реквизиты платежных поручений и другой платежной информации на АРМ главного бухгалтера |
| Срыв запланированной сделки с партнером/заказчиком (У2) | АРМ руководителя организации | Модификация информации и отправка электронных писем с недостоверной информацией от имени руководителя организации |
| Электронный почтовый ящик руководителя организации | Модификация информации и отправка электронных писем с недостоверной информацией от имени руководителя организации |
| Недоступность данных | Сервер и хранилище данных | Несанкционированная отправка команд, приводящая к несрабатыванию средств аварийной защиты |
| Программно-аппаратные средства | Несанкционированный доступ к источнику бесперебойного питания |
| Утечка персональных данных | Веб-приложение информационной системы | Несанкционированный доступ к идентификационной информации граждан, содержащейся в веб-приложении информационной системы |

# **2 Источники угроз безопасности информации**

Были определены источники угроз безопасности, собрана модель нарушителя, а также определены возможные цели реализации угроз в организации. Всё это представлено в таблице 2.1.

Таблица 2.1 – Модель нарушителя

|  |  |  |  |
| --- | --- | --- | --- |
| **№ вида** | **Вид нарушителя** | **Категории нарушителя** | **Возможные цели реализации угроз безопасности информации** |
| 1 | Отдельные физические лица (хакеры) | Внешний | Получение финансовой или иной материальной выгоды |
| 2 | Конкурирующие организации (шпионы) | Внешний | - Получение конкурентных преимуществ  - Получение финансовой или иной материальной выгоды |
| 3 | Разработчики программных, программно-аппаратных средств | Внутренний | - Получение финансовой или иной материальной выгоды  - Непреднамеренные, неосторожные или неквалифицированные действия |
| 4 | Лица, обеспечивающие функционирование систем и сетей или обеспечивающие системы оператора (администрация, охрана, уборщики и т.д.) | Внутренний | Непреднамеренные, неосторожные или неквалифицированные действия |
| 5 | Авторизованные пользователи систем и сетей АО «Россети» | Внутренний | - Получение финансовой или иной материальной выгоды  - Непреднамеренные, неосторожные или неквалифицированные действия  - Месть за ранее совершенные действия |
| 6 | Системные администраторы и администраторы безопасности | Внутренний | - Получение финансовой или иной материальной выгоды  - Месть за ранее совершенные действия  - Непреднамеренные, неосторожные или неквалифицированные действия |
| 7 | Бывшие работники | Внешний | - Получение финансовой или иной материальной выгоды  - Месть за ранее совершенные действия |

Целью выявления возможных способов реализации угроз безопасности информации является формирование предположений о потенциальных сценариях, описывающих последовательность действий индивидуальных нарушителей или групп нарушителей. Эти сценарии включают в себя алгоритмы и методы, используемые для осуществления угроз безопасности информации, а также применяемые средства.

Возможные способы реализации угроз безопасности информации подчинены структурно-функциональным характеристикам и особенностям функционирования конкретной информационной системы.

# **Заключение**

При выполнении практической работы были выявлены потенциальные объекты воздействия угроз безопасности информации и модель угроз для АО «Россети», для этого были проанализированы базы данных ФСТЭК, в результате чего были рассмотрены данные угрозы.