

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

**Модель нарушителя безопасности информации 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](#_Toc162383176)

[2. Введение 5](#_Toc162383177)

[3. Определение возможных объектов воздействия угроз безопасности информации в ФГБУ «Редакция «Российской газеты» 5](#_Toc162383178)

[4. Определение возможных объектов воздействия угроз безопасности информации в ФГБУ «Редакция «Российской газеты» 6](#_Toc162383179)

[5. Заключение 8](#_Toc162383180)

# Обозначения и сокращения

|  |  |  |
| --- | --- | --- |
| АИС | – | Автоматизированная 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 |
|  |  |  |
|  |  |  |
|  |  |  |
|  |  |  |
|  |  |  |
|  |  |  |

# Введение

В ходе оценки угроз безопасности информации должны быть определены информационные ресурсы и компоненты систем и сетей, несанкционированный доступ к которым или воздействие на которые в ходе реализации (возникновения) угроз безопасности информации может привести к негативным последствиям – объекты воздействия.

Будут выявлены источники угроз безопасности и сформулирована модель нарушителя. Источник угрозы безопасности информации – это субъект (физическое лицо, материальный объект или физическое явление), являющийся непосредственной причиной возникновения угрозы безопасности информации.

# Определение возможных объектов воздействия угроз безопасности информации в ФГБУ «Редакция «Российской газеты»

Определения объектов воздействия и видов воздействия на них представлены в таблице 1.

Таблица 1 – 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 |
| АРМы сотрудников организации | - Подмена данных, содержащих платёжную информацию, информацию о проектах  - Отправка электронных писем с недостоверной информацией или доступ к системе с ПДн |
| 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 |
| Система управления предприятием | Несанкционированный доступ к системе с последующей кражей внутренних данных компании касающихся контрактов, отчётов, бюджетов |
| 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 |

# Определение возможных объектов воздействия угроз безопасности информации в ФГБУ «Редакция «Российской газеты»

Были определены источники угроз безопасности, собрана модель нарушителя, а также определены возможные цели реализации угроз в организации. Всё это представлено в таблице 2.

Таблица 2 – Модель нарушителя

|  |  |  |  |
| --- | --- | --- | --- |
| **№** | **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 ФГБУ «Редакция «Российской газеты» | 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 (уволенные) работники (пользователи) ФГБУ «Редакция «Российской газеты» | Внешний | - Получение финансовой или иной материальной выгоды  - Месть за ранее совершенные действия |

Целью определения возможных способов реализации угроз безопасности информации является формирование предположений о возможных сценариях реализации угроз безопасности информации, описывающих последовательность (алгоритмы) действий отдельных видов нарушителей или групп нарушителей и применяемые ими методы и средства для реализации угроз безопасности информации.

Возможные способы реализации угроз безопасности информации зависят от структурно-функциональных характеристик и особенностей функционирования информационной системы.

# Заключение

В рамках практической работы были определены возможные объекты воздействия угроз безопасности информации в ФГБУ «Редакция «Российской газеты».Так же была составлена модель нарушителя. С использованием базы данных угроз с сайта ФСТЭК были рассмотрены возможные угрозы, а также возможные цели реализации этих угроз.