

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**

**АО «РОСЭНЕРГОАТОМ»**

по дисциплине

«Управление информационной безопасностью»

Группа:

ББМО-02-23

Выполнил:

Дурягин М.Р.

Москва, 2024

**Введение**

В рамках практической работы проводится оценка угроз безопасности информации с целью выявления информационных ресурсов, компонентов систем и сетей, подверженных несанкционированному доступу или воздействию, что может иметь отрицательные последствия. 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 «РОСЭНЕРГОАТОМ»**

Определения объектов воздействия и видов воздействия на них представлены в таблице 1.1.

Таблица 1.1 – 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 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 ООО «СТРОЙСТРИТ» | 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**

В ходе выполнения практической работы были выявлены потенциальные объекты воздействия угроз безопасности информации в организации АО «РОСЭНЕРГОАТОМ». Также была разработана модель нарушителя. При этом был проведен анализ базы данных угроз с официального сайта Федеральной службы по техническому и экспортному контролю (ФСТЭК), в результате чего были рассмотрены возможные угрозы, а также определены цели, стоящие за реализацией этих угроз.