|  |
| --- |
| МИНОБРНАУКИ РОССИИ |
| **Федеральное государственное бюджетное образовательное учреждение**  **высшего образования**  **«МИРЭА – Российский технологический университет»**  **РТУ МИРЭА** |

Институт кибербезопасности и цифровых технологий

Кафедра КБ-1 «Защита информации»

**ЗАЧТЕНО**

\_\_\_\_\_\_\_\_\_\_ /Е.О. Карамышева/

«\_\_\_» \_\_\_\_\_\_\_\_\_\_\_\_ 2023г.

**ОТЧЕТ ПО ПРАКТИЧЕСКОЙ РАБОТЕ №7-8**

по дисциплине

**«Организация защиты персональных данных на предприятии**»

на тему:

# «Построение модели вероятного нарушителя»

**Выполнил**

Студент 3 курса: Кутьин З.С.

Группы: БББО-05-20

Специальности: Информационная безопасность

**Введение**

В данной практической работе проведена разработка модели вероятного нарушителя безопасности персональных данных при их обработке в ИСПДн в предприятии, которое предоставляет косметологические и медицинские услуги.

**Цель работы**

Получение навыков по построению модели вероятного нарушителя безопасности персональных данных при их обработке в ИСПДн.

**Ход работы**

С учетом методических рекомендаций ФСБ России модель нарушителя должна иметь следующую структуру:

* описание нарушителей (субъектов атак);
* предположения об имеющейся у нарушителя информации об объектах атак;
* предположения об имеющихся у нарушителя средствах атак;
* описание каналов атак.

1. **Описание нарушителей (субъектов атак)**

Сначала все физические лица, имеющие доступ к техническим и программным средствам информационной системы, разделяются на следующие категории:

* категория I – лица, не имеющие права доступа в контролируемую зону информационной системы;
* категория II – лица, имеющие право постоянного или разового доступа в контролируемую зону информационной системы.

Далее все потенциальные нарушители подразделяются на:

* внешних нарушителей, осуществляющих атаки из-за пределов контролируемой зоны информационной системы;
* внутренних нарушителей, осуществляющих атаки, находясь в пределах контролируемой зоны информационной системы.

Таблица 1 – Описание потенциальных нарушителей.

|  |  |  |  |  |
| --- | --- | --- | --- | --- |
| Вероятный нарушитель | Категория | Тип | Описание привилегированных пользователей | Обоснование исключения лиц категории II из числа потенциальных нарушителей |
| Клиенты салона | Категория II | Внешний нарушитель |  |  |
| Рядовые сотрудники | Категория  II | Внутренний нарушитель |  |  |
| Сотрудники, обеспечивающие функционирование технических средств | Категория II | Внутренний нарушитель | Это внутренние сотрудники, которые имеют расширенные полномочия для работы с корпоративными ресурсами. На них возложены задачи по администрированию программно-аппаратных средств, СКЗИ и баз данных ИСПДн. | Указанные лица назначаются из числа особо доверенных лиц и осуществляют техническое обслуживание технических и программных средств. Данная категория лиц заинтересована в сохранении свойств безопасности защищаемых и обслуживаемых объектов. |
| Сотрудники других организаций, осуществляющие поставку, ремонт ПО и/или технических средств | Категория II | Внутренний нарушитель | Это сторонние специалисты, которые имеют расширенные полномочия для работы с корпоративными ресурсами, в частности для их установки, настройки, аудита и обслуживания. | Указанные лица заинтересованы в сохранении свойств безопасности поставляемых и обслуживаемых технических средств. |
| Конкуренты | Категория I | Внешний нарушитель |  |  |

В свою очередь сговор конкурентной фирмы и рядовых сотрудников (клиентов) может быть обусловлен идеологическими и политическими взглядами, а также сложившейся экономической ситуацией.

1. **Предположения об имеющейся у нарушителя информации об объектах атак**

Предполагается, что потенциальные нарушители обладают всей информацией, необходимой для подготовки и проведения атак, за исключением информации, доступ к которой со стороны нарушителя исключается системой защиты информации.

Таблица 2 – Предположение о сведениях недоступных вероятному нарушителю.

|  |  |
| --- | --- |
| Вероятный нарушитель | Перечень сведений, в отношении которых предполагается, что  они нарушителю недоступны |
| Клиенты салона | * содержание технической документации на технические и программные компоненты * сведения о линиях связи, по которым передается защищаемая информация * долговременные ключи криптосредства * все сети связи, работающие на едином ключе |
| Рядовые сотрудники | * содержание технической документации на технические и программные компоненты * долговременные ключи криптосредства * все сети связи, работающие на едином ключе |
| Конкуренты | * содержание технической документации на технические и программные компоненты * сведения о линиях связи, по которым передается защищаемая информация * все сети связи, работающие на едином ключе |

Полный доступ к содержанию технической документации на технические и программные компоненты, всем сетям связи, работающим на едином ключе, имеет только ответственный пользователь, такой как администратор ИСПДн и директор фирмы.

1. **Предположения об имеющихся у нарушителя средствах атак**

Предполагается, что нарушитель имеет все необходимые для проведения атак по доступным ему каналам атак средства, возможности которых не превосходят возможности аналогичных средств атак на информацию, содержащую сведения, составляющие государственную тайну.

Таблица 3 – Перечень средств атак, предположительно имеющихся у нарушителя.

|  |  |
| --- | --- |
| Вероятный нарушитель | Перечень средств атак, предположительно имеющихся у нарушителя |
| Клиенты салона | * доступные в свободной продаже аппаратные компоненты криптосредства * доступные в свободной продаже технические средства и программное обеспечение * штатные средства за пределами КЗ |
| Рядовые сотрудники | * доступные в свободной продаже аппаратные компоненты криптосредства * доступные в свободной продаже технические средства и программное обеспечение * штатные средства внутри КЗ |
| Конкуренты | * лабораторные исследования криптосредств, используемых за пределами КЗ * специально разработанные технические средства и программное обеспечение * штатные средства за пределами КЗ * доступные в свободной продаже технические средства и программное обеспечение |

1. **Описание каналов атак**

Угрозы безопасности реализуются в результате образования канала реализации угрозы, возникающего между источником угрозы и носителем ПДн, что создает необходимые условия для возможного нарушения безопасности ПДн (несанкционированный или случайный доступ).

Таблица 4 – Основные каналы атак.

|  |  |
| --- | --- |
| Основные каналы атак | Вероятный нарушитель |
| Акустический, визуальный и физический канал доступа | Клиенты, Рядовые сотрудники, Конкуренты |
| Машинные носители информации | Рядовые сотрудники |
| Носители информации, выведенные из употребления | Рядовые сотрудники, Конкуренты |
| Технические каналы утечки | Конкуренты |
| Информационные и управляющие интерфейсы СВТ | Клиенты, Рядовые сотрудники, Конкуренты |

1. **Определение типа нарушителя**

Таблица 5 – Тип вероятного нарушителя.

|  |  |
| --- | --- |
| Вероятный нарушитель | Тип нарушителя |
| Клиенты салона красоты | H1 |
| Рядовые сотрудники | H2 |
| Конкуренты | H4 |

**Вывод**

Я научился построению модели вероятного нарушителя и, исходя из моей работы можно сделать вывод, что наиболее вероятным нарушителем является конкурент компании.