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

ИКБ направление «Кибербразведка и противодействие угрозам с применением технологий искусственного интеллекта» 10.04.01

Кафедра КБ-4 «Интеллектуальные системы информационной безопасности»

Модель нарушителя безопасности информации

по дисциплине

«Управление информационной безопасностью»

Группа:
ББМО-02-22
Выполнил:
Щелкушкин Е.Р.

Проверил:
Пимонов Р.В.

Москва 2023

4. Возможные объекты воздействия угроз безопасности информации

Таблица 1 – Возможные цели реализации угроз безопасности информации нарушителями

№	Виды нарушителя	Категории нарушителя	Возможные цели реализации угроз безопасности информации
1	Отдельные физические лица (хакеры)	Внешний	Получение финансовой или иной материальной выгоды. Любопытство или желание самореализации (подтверждение статуса)
2	Лица, привлекаемые для установки, настройки, испытаний, пусконаладочных и иных видов работ	Внутренний	Получение финансовой или иной материальной выгоды. Непреднамеренные, неосторожные или неквалифицированные действия. Получение конкурентных преимуществ
3	Авторизованные пользователи систем и сетей	Внутренний	Получение финансовой или иной материальной выгоды. Любопытство или желание самореализации (подтверждение статуса). Месть за ранее совершенные действия. Непреднамеренные, неосторожные или неквалифицированные действия
4	Системные администраторы и администраторы безопасности	Внутренний	Получение финансовой или иной материальной выгоды. Любопытство или желание самореализации (подтверждение статуса). Месть за ранее совершенные действия. Непреднамеренные, неосторожные или неквалифицированные действия

Таблица 2 – Оценка целей реализации нарушителями угроз безопасности информации в зависимости от возможных негативных последствий и видов ущерба от их реализации

Виды нарушителей	**Возможные цели реализации угроз безопасности информации**			**Соответствие целей видам риска (ущерба) и возможным негативным последствиям**
	Нанесение ущерба физическому лицу	Нанесение ущерба юридическому лицу,	Нанесение ущерба государству	

		индивидуальному предпринимателю		
Отдельные физические лица (хакеры)	Желание самореализоваться	Получение финансовой выгоды за счет кражи и коммерческой тайны	-	Нарушение личной, семейной тайны, утрата чести и доброго имени; утечка коммерческой тайны; потеря клиентов
Лица, привлекаемые для установки, настройки, испытаний, пусконаладочных и иных видов работ	Передача информации о физическом лице третьим лицам	Передача информации о физическом/юридическом лице третьим лицам, а также о структуре внутренней системы	-	Нарушение функционирования
Авторизованные пользователи систем и сетей	Непреднамеренные, неосторожные или неквалифицированные действия	-	-	Финансовый, иной материальный ущерб физическим лицам
Системные администраторы и администраторы безопасности	Месть за ранее совершенные действия	Любопытство или желание самореализации	Получение финансовой или иной материальной выгоды при вступлении в сговор с преступной группой	Финансовый, иной материальный ущерб физическим лицам; невозможность заключения договоров, соглашений; утечка информации ограниченного доступа

Таблица 3 – Характеристики возможных нарушителей

№	Возможный вид нарушителя	Категория	Уровень возможностей	Актуальность

1	Отдельные физические лица (хакеры)	Внешний	H2. Нарушитель, обладающий базовыми повышенными возможностями	Да
2	Лица, привлекаемые для установки, настройки, испытаний, пусконаладочных и иных видов работ	Внутренний / Внешний	H1. Нарушитель, обладающий базовыми возможностями	Да
3	Авторизованные пользователи систем и сетей	Внутренний	H1. Нарушитель, обладающий базовыми возможностями	Да
4	Системные администраторы и администраторы безопасности	Внутренний	H2. Нарушитель, обладающий базовыми повышенными возможностями	Да

5. Актуальные угрозы информационной безопасности

Таблица 4 – Перечень рассматриваемых нарушителей

№	Вид нарушителя	Возможные цели реализации угроз безопасности информации	Предположение об отнесении к числу возможных нарушителей
1	Отдельные физические лица (хакеры)	Получение финансовой или иной материальной выгоды. Любопытство или желание самореализации.	Возможные цели реализации угроз безопасности информации предполагают наличие нарушителя

2	Конкурирующие организации	Получение конкурентных преимуществ. Получение финансовой или иной материальной выгоды.	Не имеют достаточной мотивации для осуществления деятельности, связанной с нарушением характеристик безопасности конфиденциальной информации, обрабатываемой в Подсистеме
3	Поставщики вычислительных услуг, услуг связи	Получение финансовой или иной материальной выгоды. Непреднамеренные, неосторожные или неквалифицированные действия.	Не имеют достаточной мотивации для осуществления деятельности, связанной с нарушением характеристик безопасности конфиденциальной информации, обрабатываемой в Подсистеме
4	Лица, привлекаемые для установки, настройки, испытаний, пусконаладочных и иных видов работ	Получение финансовой или иной материальной выгоды. Непреднамеренные, неосторожные или неквалифицированные действия.	Возможные цели реализации угроз безопасности информации предполагают наличие нарушителя
5	Лица, обеспечивающие функционирование систем и сетей или обеспечивающие системы оператора (администрация, охрана, уборщики и т. д.)	Получение финансовой или иной материальной выгоды. Непреднамеренные, неосторожные или неквалифицированные действия.	Не имеют достаточной мотивации для осуществления деятельности, связанной с нарушением характеристик безопасности
6	Системные администраторы и администратор	Получение финансовой или иной материальной выгоды. Месть за ранее совершенные действия. Непреднамеренные, неосторожные или неквалифицированные действия	Возможные цели реализации угроз безопасности информации

			предполагают наличие нарушителя
	Бывшие работники (пользователи)	Получение финансовой или иной материальной выгоды. Месть за ранее совершенные действия.	Не имеют достаточной мотивации для осуществления деятельности, связанной с нарушением характеристик безопасности конфиденциальной информации.