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-01-22
Выполнила:
Огольцова Н.Д.

Проверил:
Пимонов Р.В.

Москва 2023

1. Возможные объекты воздействия угроз безопасности информации

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

Исходными данными для определения возможных объектов воздействия являются:

а) общий перечень угроз безопасности информации, содержащихся в банке данных угроз безопасности информации ФСТЭК России (bdu.fstec.ru), модели угроз безопасности информации, разрабатываемые ФСТЭК России в соответствии с подпунктом 4 пункта 8 Положения о Федеральной службе по техническому и экспортному контролю, утвержденного Указом Президента Российской Федерации от 16 августа 2004 г. № 1085, а также отраслевые (ведомственные, корпоративные) модели угроз безопасности информации;

б) документация на сети и системы (в части сведений о составе и архитектуре, о группах пользователей и уровне их полномочий и типах доступа, внешних и внутренних интерфейсах);

в) негативные последствия от реализации (возникновения) угроз безопасности информации.

На основе анализа исходных данных и результатов инвентаризации систем и сетей определены следующие группы информационных ресурсов и компонентов систем и сетей, которые могут являться объектами воздействия:

а) информация (данные), содержащаяся в системах и сетях (защищаемая информация, информация о конфигурации системы и сети);

б) программно-аппаратные средства обработки и хранения информации (ПЭВМ, сервера);

в) машинные носители информации, содержащие как защищаемую информацию, так и аутентификационную информацию;

г) телекоммуникационное оборудование (в том числе программное обеспечение для управления телекоммуникационным оборудованием);

д) средство защиты информации;

е) объекты файловой системы.

В отношении каждого объекта воздействия определялись виды воздействия на него, которые могут привести к негативным последствиям. Рассматриваемые виды воздействия представлены в Таблице 1.

Идентификатор	Вид воздействия
ВВ.1	Утечка (перехват) конфиденциальной информации или отдельных данных (нарушение конфиденциальности)
ВВ.2	Несанкционированный доступ к компонентам, защищаемой информации, системным, конфигурационным, иным служебным данным
ВВ.3	Отказ в обслуживании компонентов (нарушение доступности)
ВВ.4	Несанкционированная модификация, подмена, искажение защищаемой информации, системных, конфигурационных, иных служебных данных (нарушение целостности)
ВВ.5	Нарушение функционирования (работоспособности) программно-аппаратных средств обработки, передачи и хранения информации

2. Источники угроз безопасности информации

Исходными данными для определения возможных актуальных нарушителей являются:

а) общий перечень угроз безопасности информации, содержащихся в банке данных угроз безопасности информации ФСТЭК России (bdu.fstec.ru), модели угроз безопасности информации, разрабатываемые ФСТЭК России в соответствии с подпунктом 4 пункта 8 Положения о Федеральной службе по техническому и экспортному контролю, утвержденного Указом Президента Российской Федерации от 16 августа 2004 г. № 1085, а также отраслевые (ведомственные, корпоративные) модели угроз безопасности информации;

б) документация на сети и системы (в части сведений о составе и архитектуре, о группах пользователей и уровне их полномочий, типах доступа, внешних и внутренних интерфейсах);

в) негативные последствия от реализации (возникновения) угроз безопасности информации;

г) объекты воздействия угроз безопасности информации и виды воздействия на них.

На основе анализа исходных данных, а также результатов оценки возможных целей реализации нарушителями угроз безопасности информации определен перечень рассматриваемых нарушителей, актуальных для систем и сетей. Данный перечень указан в Таблице 2.

Вид нарушителя	Возможные цели реализации угроз безопасности информации	Предположение об отнесении к числу возможных нарушителей
Отдельные физические лица (хакеры)	Получение финансовой или иной материальной выгоды. Любопытство или желание самореализации.	Возможные цели реализации угроз безопасности информации предполагают наличие нарушителя
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

Вид нарушителя	Возможные цели реализации угроз безопасности информации	Предположение об отнесении к числу возможных нарушителей
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
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
Вид нарушителя	Возможные цели реализации угроз безопасности информации	Предположение об отнесении к числу возможных нарушителей
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

Вид нарушителя	Возможные цели реализации угроз безопасности информации	Предположение об отнесении к числу возможных нарушителей
		конфиденциальной информации, обрабатываемой в Подсистеме.
Авторизованные пользователи систем и сетей	Любопытство или желание самореализации (подтверждение статуса). Месть за ранее совершенные действия. Непреднамеренные, неосторожные или неквалифицированные действия.	Возможные цели реализации угроз безопасности информации предполагают наличие нарушителя.
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.