**Модель нарушителя «защищенного чата»**

|  |  |  |  |  |  |
| --- | --- | --- | --- | --- | --- |
| Тип нарушителя | Расположение | Мотив нарушения | Квалификация | Техническая оснащенность | Вероятность проявления |
| Специальные службы Иностранных государств (блоков государств) | Внешний,  внутренний | Нанесение ущерба государству, отдельным его сферам деятельности или секторам экономики. Дискредитация или дестабилизация деятельности органов государственной власти, организаций | Высокая | Высокая | Низкая |
| Террористические, экстремистские группировки | Внешний | Нанесение ущерба государству, отдельным его сферам деятельности или секторам экономики. Совершение террористических актов. Идеологические или политические мотивы. Дестабилизация деятельности органов государственной власти, организаций | Средняя | Низкая | Низкая |
| Преступные группы (криминальные структуры) | Внешний | Причинение имущественного ущерба путем мошенничества или иным преступным путем. Выявление уязвимостей с целью их дальнейшей продажи и получения финансовой выгоды | Высокая | Средняя | Высокая |
| Внешние субъекты (физические лица) | Внешний | Идеологические или политические мотивы. Причинение имущественного ущерба путем мошенничества или иным преступным путем. Любопытство или желание самореализации (подтверждение статуса). Выявление уязвимостей с целью их дальнейшей продажи и получения финансовой выгоды | Низкая | Низкая | Высокая |
| Конкурирующие организации | Внешний | Получение конкурентных преимуществ. Причинение имущественного ущерба путем обмана или зло употребления доверием | Средняя | Низкая | Высокая |
| Разработчики, производители, поставщики программных, технических и Программно- технических средств | Внешний | Внедрение дополнительных функциональных возможностей в программное обеспечение или программно-технические средства на этапе разработки. Причинение имущественного ущерба путем обмана или злоупотребления доверием. Непреднамеренные, неосторожные или неквалифицированные действия | Высокая | Высокая | Низкая |
| Лица, привлекаемые для установки, наладки, монтажа, пусконаладочных и иных видов работ | Внутренний | Причинение имущественного ущерба путем обмана или злоупотребления доверием. Непреднамеренные, неосторожные или неквалифицированные действия | Средняя | Низкая | Средняя |
| Лица, обеспечивающие функционирование информационных систем или обслуживающие инфраструктуру оператора (администрация, охрана, уборщики и т.д.) | Внутренний | Причинение имущественного ущерба путем обмана или злоупотребления доверием. Непреднамеренные, неосторожные или неквалифицированные действия | Низкая | Низкая | Средняя |
| Пользователи информационной системы | Внутренний | Причинение имущественного ущерба путем мошенничества или иным преступным путем. Любопытство или желание самореализации (подтверждение статуса). Месть за ранее совершенные действия. Непреднамеренные, неосторожные или неквалифицированные действия | Низкая | Низкая | Высокая |
| Администраторы информационной системы и администраторы безопасности | Внутренний | Причинение имущественного ущерба путем мошенничества или иным преступным путем. Любопытство или желание самореализации (подтверждение статуса). Месть за ранее совершенные действия. Выявление уязвимостей с целью их дальнейшей продажи и получения финансовой выгоды. Непреднамеренные, неосторожные или неквалифицированные действия | Высокая | Средняя | Средняя |
| Бывшие работники (пользователи) | Внешний | Причинение имущественного ущерба путем мошенничества или иным преступным путем. Месть за ранее совершенные действия | Высокая | Средняя | Средняя |

**Модель угроз безопасности «защищенного чата»**

|  |  |  |  |
| --- | --- | --- | --- |
| Наименование угрозы | Возможность реализации | Опасность угрозы | Меры по противодействию угрозе |
| Получение несанкционированного физического доступа к ЭВМ-клиентам | Высокая | Высокая | Запрос пароля при входе в ЭВМ-клиент;  Запрос пароля при запуске программы;  Запрет внешних подключений удаленного рабочего стола, специализированных программ удаленного управления; |
| Получение несанкционированного физического доступа к каналам связи с дальнейшим подключением несанкционированных устройств | Высокая | Высокая | Запрет внешних подключений;  Запрет беспроводных подключений;  Идентификация устройств по уникальным значениям и использование защитных механизмов блокировки неизвестных устройств |
| Заражение компьютеров пользователей программы | Низкая | Высокая | Использование антивирусного ПО |
| Перехват информации при передаче по каналам связи | Высокая | Средняя | Запрет внешних подключений;  Запрет беспроводных подключений; Шифрование передаваемых пакетов с помощью программы |
| Получение доступа к файлам пользователей | Низкая | Низкая | Разграничение доступа к файлам клиентов; |
| Получение доступа к файлу ключа | Средняя | Средняя | Шифрование файла |
| Создание слабого пароля | Средняя | Высокая | Установка высоких требований к сложности пароля для входа в программу |
| Непреднамеренное удаление файла ключа | Низкая | Высокая | Перемещение удаленных файлов в «корзину» |