**Виды возможных угроз**

|  |  |
| --- | --- |
| **Категория** | **Угрозы / Атаки** |
| *Проверка Ввода* | [Переполнение буфера](https://ru.wikipedia.org/wiki/%D0%9F%D0%B5%D1%80%D0%B5%D0%BF%D0%BE%D0%BB%D0%BD%D0%B5%D0%BD%D0%B8%D0%B5_%D0%B1%D1%83%D1%84%D0%B5%D1%80%D0%B0);  [внедрение SQL-кода](https://ru.wikipedia.org/wiki/%D0%92%D0%BD%D0%B5%D0%B4%D1%80%D0%B5%D0%BD%D0%B8%D0%B5_SQL-%D0%BA%D0%BE%D0%B4%D0%B0); стандартизация (канонизация) |
| *Фальсификация программного обеспечения* | Злоумышленник изменяет поведение приложения для выполнения несанкционированных действий, путем бинарного исправления, замены кода или его расширения |
| [*Аутентификация*](https://ru.wikipedia.org/wiki/%D0%90%D1%83%D1%82%D0%B5%D0%BD%D1%82%D0%B8%D1%84%D0%B8%D0%BA%D0%B0%D1%86%D0%B8%D1%8F) | Кража учетных данных |
| [*Авторизация*](https://ru.wikipedia.org/wiki/%D0%90%D0%B2%D1%82%D0%BE%D1%80%D0%B8%D0%B7%D0%B0%D1%86%D0%B8%D1%8F) | [Повышение привилегий](https://ru.wikipedia.org/wiki/%D0%9F%D0%BE%D0%B2%D1%8B%D1%88%D0%B5%D0%BD%D0%B8%D0%B5_%D0%BF%D1%80%D0%B8%D0%B2%D0%B8%D0%BB%D0%B5%D0%B3%D0%B8%D0%B9); раскрытие конфиденциальных данных; подделка данных |
| *Управление конфигурацией* | Несанкционированный доступ к интерфейсам администрирования; несанкционированный доступ к файлам настроек; поиск текстовых данных конфигурации; чрезмерно привилегированные процессы и службы |
| *Конфиденциальная информация* | Доступ к чувствительному коду или данным в хранилище; подслушивание сети; внедрение вредоносного кода / данных |
| *Управление сеансом* | [Похищение сеанса](https://ru.wikipedia.org/wiki/TCP_hijacking); [атака повторного воспроизведения](https://ru.wikipedia.org/wiki/%D0%90%D1%82%D0%B0%D0%BA%D0%B0_%D0%BF%D0%BE%D0%B2%D1%82%D0%BE%D1%80%D0%BD%D0%BE%D0%B3%D0%BE_%D0%B2%D0%BE%D1%81%D0%BF%D1%80%D0%BE%D0%B8%D0%B7%D0%B2%D0%B5%D0%B4%D0%B5%D0%BD%D0%B8%D1%8F); [атака «человек посередине»](https://ru.wikipedia.org/wiki/%D0%90%D1%82%D0%B0%D0%BA%D0%B0_%D0%BF%D0%BE%D1%81%D1%80%D0%B5%D0%B4%D0%BD%D0%B8%D0%BA%D0%B0) |
| *Аудит и вход в систему* | Пользователь запрещает выполнение операции; злоумышленник использует приложение без следа; злоумышленник скрывает свои следы |

**Характер происхождения угроз**

Преднамеренные воздействия - это целенаправленные действия злоумышленника. В качестве злоумышленника могут выступать служащий, посетитель, конкурент, наемник. Действия нарушителя могут быть обусловлены разными мотивами. Это могут быть умышленные факторы:

- хищение носителей информации;

- подключение к каналам связи;

- перехват электромагнитных излучений;

- несанкционированный доступ;

- разглашение информации;

- копирование данных.

Причинами случайных воздействий при эксплуатации могут быть естественные факторы, к которым относятся:

- несчастные случаи (пожары, аварии, взрывы);

- стихийные бедствия (ураганы, наводнения, землетрясения);

- ошибки в процессе обработки информации (ошибки пользователя, оператора, сбои аппаратуры).

Угрозы, связанные с сервером.

Серверы меньше подвержены атакам, поскольку они, как правило, работают в контролируемых условиях, обслуживаются квалифицированными администраторами и обладают одним или несколькими уровнями защиты.

**Источники появления угроз**

* Человеческий фактор – нанятый работник выдать конфиденциальную информацию в руки мошенника, ошибиться при передаче данных оставив дыру в защите.
* Несанкционированное ПО – заражение компьютера вирусами.
* Технические устройства;
* Модели, алгоритмы, программы;
* Технологические схемы обработки;
* Внешняя среда

**Потенциально возможные злоумышленные действия.**

Угрозы и злоумышленные действия можно рассматривать с точки зрения воздействия их на такие качества объекта(информационной системы), как готовность, надежность и конфиденциальность.

Готовность-способность информационной системы обеспечить законным пользователям условия доступа к ресурсам в соответствии с принятым режимом работы.

Конфиденциальность - способность системы обеспечить целостность и сохранность информации ее законных пользователей.

Надежность-способность системы обеспечить информационные потребности только законным пользователям в рамках их интересов.

В общем плане к злоумышленным действиям относятся: похищения и угрозы похищения сотрудников и персонала, убийства, психологический террор, угрозы, шантаж, грабежи.

Преступные посягательства в отношении помещений, зданий и персонала проявляются в виде: взрывов, поджогов, нападений, вторжений и захватов.

Осуществление угроз информационным ресурсам может быть произведено:

-через имеющиеся агентурные источники в органах государственного управления, коммерческих структур, имеющих доступ к конфиденциальной информации;

-через подкуп лиц, работающих с основными документами;

-путем перехвата информации в средствах и системах связи и хранения информации при несанкционированном доступе.

**Рекомендации повышения защищенности ИС**

* Все используемые средства для защиты должны быть доступными для пользователей и простыми для технического обслуживания.
* Каждого пользователя нужно обеспечить минимальными привилегиями, необходимыми для выполнения конкретной работы.
* Система защиты должна быть автономной.
* Необходимо предусмотреть возможность отключения защитных механизмов в ситуациях, когда они являются помехой для выполнения работ.
* Разработчики системы безопасности должны учитывать максимальную степень враждебности окружения, то есть предполагать самые наихудшие намерения со стороны злоумышленников и возможность обойти все защитные механизмы.
* Наличие и место расположение защитных механизмов должно быть конфиденциальной информацией.
* Организация обеспечения безопасности информационных банковских систем основывается на тех же принципах защиты и предполагает постоянную модернизацию защитных функций, поскольку эта сфера постоянно развивается и совершенствуется. Казалось бы, еще недавно созданные новые защитные системы со временем становятся уязвимыми и недейственными, вероятность их взлома с каждым годом возрастает.