Способы классификации угроз

написано Александр Астахов | 10 июня, 2023

Существуют различные способы классификации угроз безопасности: по объекту воздействия, по источнику угрозы, способам ее осуществления, возможным последствиям и видам ущерба. Одновременно могут использоваться несколько критериев классификации, например, угрозы, классифицированные по объекту воздействия, дополнительно, внутри каждого класса, могут классифицироваться по видам ущерба и источникам угрозы.

По виду активов, на которые они направлены (объектам воздействия), угрозы делятся на:

- угрозы, направленные против информационных активов;
- угрозы, направленные против программного обеспечения;
- угрозы, направленные против технических средств;
- угрозы кадровым ресурсам;
- угрозы помещениям организации.

В конечном итоге все перечисленные классы угроз, за исключением последнего, могут оказывать прямое влияние на безопасность информационных активов.

По источнику угрозы можно разделить, например, на следующие классы:

- угрозы со стороны различных классов внешних нарушителей;
- угрозы со стороны различных классов внутренних нарушителей;
- угрозы со стороны партнеров и подрядчиков;
- антропогенные катастрофы (терроризм, взрывы, массовые беспорядки);
- техногенные аварии (сбои технических средств);
- природные катаклизмы (землетрясение, наводнение, ураганы и т.п.);

- несчастные случаи (пожар, обрушение здания и т.п.).

По типу нарушения угрозы можно разделить на следующие классы:

- угрозы нарушения конфиденциальности информации;
- угрозы нарушения целостности информации;
- угрозы нарушения доступности информации;
- угрозы отказа от совершенных действий с информацией (угрозы неотказуемости);
- угрозы, связанные с невозможностью установления авторства электронных документов (угрозы аутентичности);
- угрозы нарушения требований законодательства.

Далее мы более подробно рассмотрим некоторые основные классы угроз безопасности.

Угрозы, реализуемые при помощи программных средств

Угрозы информационной безопасности, *реализуемые с использованием программных средств*, – наиболее многочисленный класс угроз в отношении конфиденциальности, целостности и доступности информационных активов, связанный с получением внутренними или внешними нарушителями несанкционированного логического доступа к информации, а также блокированием или разрушением этой информации с использованием возможностей, предоставляемых общесистемным и прикладным программным обеспечением.

К этому классу угроз относится, например, следующее:

- использование ошибок проектирования, кодирования, либо конфигурации для получения НСД;
- использование закладок в ПО, оставленных для отладки, либо умышленно внедренных;
- сбои в работе средств защиты информации;
- маскарад, перехват паролей или взлом паролей пользователей;

- нецелевое использование ПО;
- анализ сетевого трафика с целью перехвата информации;
- замена, вставка, удаление или изменение данных пользователей в информационном потоке;
- ошибки пользователей и технического персонала;
- внедрение вредоносного ПО;
- утечка конфиденциальной информации по электронным каналам связи (электронная почта, системы мгновенных сообщений и т.п.) либо на внешние устройства и носители информации;
- и т.п.

Большинство рассматриваемых в этом классе угроз реализуется путем осуществления локальных или удаленных атак на информационные активы системы внутренними и внешними нарушителями. Результатом успешного осуществления этих угроз становится получение НСД к информации электронного архива, управляющей информации, хранящимся на рабочих местах администраторов, конфигурационной информации активного сетевого оборудования, а также к данным, передаваемым по каналам связи.

Угрозы утечки информации по техническим каналам

Утечка информации по техническим каналам связи – это специфический класс угроз, требующий для своей реализации специальных навыков и оборудования для проведения технической разведки. Такие методы пускаются в ход, когда перехватываемая информации имеет очень большую ценность, что характерно для деятельности разведслужб.

К данному классу угроз относится следующее:

- побочные электромагнитные излучения;
- наводки сигнала на провода и линии связи, заземления, электропитания;
- радиоизлучения, модулированные информативным сигналом,

паразитные излучения;
- радиоизлучения, обусловленные воздействием на технические средства высокочастотных сигналов, создаваемых при помощи разведывательной аппаратуры;
- аппаратные закладки;
- акустическое излучение речевого сигнала;
- виброакустические излучения речевого сигнала;
- просмотр информации с экранов дисплеев при помощи оптических средств;
- телевизионная и фотографическая разведка.

Угрозы в отношении программных средств

Программное обеспечение выступает в трех ипостасях. Во-первых, оно является средством обработки информации, которое может использоваться для нарушения безопасности информационных активов. Во-вторых, исходные тексты и исполняемые файлы программ сами по себе являются информационными активами, подверженными тем же угрозам безопасности, что и любые другие активы. В-третьих, программное обеспечение выступает в качестве объекта интеллектуальной собственности, нуждающегося в юридической защите.

В отношении *программных средств* могут реализовываться следующие виды угроз:

- порча ПО и резервных копий;
- внесение несанкционированных изменений в исходные тесты ПО;
- использование нелицензионного ПО;
- нарушение лицензионных соглашений;
- нарушение конфиденциальности программных кодов.

Угрозы техническим средствам

К данному классу относятся угрозы доступности, целостности и, в некоторых случаях, конфиденциальности информации, хранимой,

обрабатываемой и передаваемой по каналам связи, связанные с повреждениями и отказами технических средств системы и повреждением линий связи.

В этом классе целесообразно рассмотреть следующие *основные виды угроз*:

- умышленное или неумышленное физическое повреждение технических средств внутренними нарушителями;
- физическое повреждение сетевого и каналообразующего оборудования внутренними нарушителями;
- физическое повреждение линий связи внешними или внутренними нарушителями;
- перебои в системе электропитания;
- отказы технических средств;
- установка непроверенных технических средств или замена вышедших из строя аппаратных компонентов на неидентичные компоненты;
- хищение носителей конфиденциальной информации внутренними нарушителями вследствие отсутствия контроля за их использованием и хранением.

Источниками угроз в отношении технических средств могут служить:

- внутренние нарушители, имеющие доступ к системному оборудованию и линиям связи;
- внешние нарушители, имеющие доступ к линиям связи;
- пожар;
- наводнение;
- другие стихийные бедствия.

Подробный перечень угроз безопасности, обычно рассматриваемых при оценке информационных рисков, приведен в Приложении № 5.