Приложение 5. Перечень типовых угроз информационной безопасности

написано Александр Астахов | 11 июня, 2023

Следующий перечень содержит некоторые примеры угроз и уязвимостей, связанных с целями и механизмами контроля из ISO/IEC 27002:2005. Этот перечень не является исчерпывающим и должен рассматриваться только в качестве примера, однако его более чем достаточно для проведения высокоуровневой оценки рисков.

Один из наиболее важных принципов заключается в том, что организация должна самостоятельно выбрать подходы к оценке и управлению рисками, которые должным образом учитывают и идентифицируют полный диапазон угроз и уязвимостей, имеющих отношение к ее бизнес-окружению и могут включать все или часть угроз и уязвимостей, приведенных в следующем перечне.

Физические угрозы

- Физический несанкционированный доступ в помещения организации, в кабинеты и серверные комнаты, к оборудованию, бумажным документам, запоминающим устройствам, носителям информации и т.п.
- Кража или повреждение компьютерного оборудования и носителей информации инсайдерами.
- Кража или повреждение компьютерного оборудования и носителей информации внешними злоумышленниками.
- Постороннее лицо может получить физический доступ к комплексу средств защиты с целью переконфигурирования либо создания возможности обхода средств защиты.
- Кража бумажных документов инсайдерами.
- Кража бумажных документов внешними злоумышленниками.

Нецелевое использование компьютерного оборудования и сети Интернет сотрудниками организации

- Злоупотребление средствами аудита.
- Злоупотребление средствами обработки информации.
- Злоупотребление ресурсами или активами.
- Несанкционированное использование программного обеспечения.
- Использование сетевых средств несанкционированным образом.
- Неосторожное или умышленное злоупотребление оборудованием по причине отсутствия разделения обязанностей или их неисполнения.

Угрозы утечки конфиденциальной информации

- Утечка конфиденциальной информации из сети по каналам связи (e-mail, web, chat/IM и т.п.).
- Утечка конфиденциальной информации на мобильных устройствах, носителях информации, ноутбуках и т.п.
- Прослушивание внешних каналов связи злоумышленниками.
- Нарушение конфиденциальности данных, передаваемых по линиям связи, проходящим вне контролируемой зоны, осуществляемого внешними нарушителями путем пассивного прослушивания каналов связи (подключение к каналам связи и перехват информации возможен во многих местах).
- Нарушение конфиденциальности данных, передаваемых по линиям связи, проходящим внутри контролируемой зоны, осуществляемого внутренними нарушителями путем пассивного прослушивания каналов связи с использованием специализированных программных средств («снифферов»).

- Аутентификационная информация или конфиденциальные данные могут быть модифицированы либо перехвачены вследствие активного или пассивного прослушивания в системе внешних коммуникаций либо во внутренней сети.
- Перехват информации на линиях связи путем использования различных видов анализаторов сетевого трафика.
- Замена, вставка, удаление или изменение данных пользователей в информационном потоке.
- Перехват информации, например пользовательских паролей, передаваемой по каналам связи, с целью ее последующего использования для обхода средств сетевой аутентификации.
- Статистический анализ сетевого трафика (например, наличие или отсутствие определенной информации, частота передачи, направление, типы данных и т.п.
- Неумышленное раскрытие конфиденциальной информации сотрудниками компании.
- Несанкционированное раскрытие информации о местонахождении площадок/зданий/офисов, содержащих критичные или конфиденциальные средства обработки информации.
- Раскрытие конфиденциальной информации подрядчиками или партнерами компании.

Угрозы утечки информации по техническим каналам

- Побочные электромагнитные излучения информативного сигнала от технических средств и линий передачи информации.
- Наводки информативного сигнала, обрабатываемого техническими средствами, на провода и линии, выходящие за пределы контролируемой зоны предприятия (учреждения), в том числе на цепи заземления и электропитания.
- Изменения тока потребления, обусловленные обрабатываемыми техническими средствами информативными

сигналами

- Изменения тока потребления, обусловленные обрабатываемыми техническими средствами, информативными сигналами.
- Радиоизлучения, модулированные информативным сигналом, возникающие при работе различных генераторов, входящих в состав технических средств, или при наличии паразитной генерации в узлах (элементах) технических средств.
- Электрические сигналы или радиоизлучения, обусловленные воздействием на технические средства высокочастотных сигналов, создаваемых с помощью разведывательной аппаратуры, и модуляцией их информативным сигналом (облучение, «навязывание»).
- Радиоизлучения или электрические сигналы от внедренных в технические средства и выделенные помещения специальных электронных устройств перехвата информации («закладок»), модулированные информативным сигналом.
- Радиоизлучения или электрические сигналы от электронных устройств перехвата информации, подключенных к каналам связи или техническим средствам обработки информации.
- Акустическое излучение информативного речевого сигнала или сигнала, обусловленного функционированием технических средств обработки информации.
- Электрические сигналы, возникающие посредством преобразования информативного сигнала из акустического в электрический за счет микрофонного эффекта и распространяющиеся по проводам и линиям передачи информации.
- Вибрационные сигналы, возникающие посредством преобразования информативного акустического сигнала при воздействии его на строительные конструкции и инженерно-технические коммуникации выделенных помещений.
- Просмотр информации с экранов дисплеев и других средств ее отображения с помощью оптических средств.
- Акустическая разведка, обеспечивающая добывание информации, содержащейся непосредственно в произносимой либо воспроизводимой речи (акустическая речевая

разведка), с использованием аппаратуры, регистрирующей акустические (в воздухе) и виброакустические (в упругих средах) волны, а также электромагнитные излучения и электрические сигналы, возникающие за счет акустоэлектрических преобразований в различных технических средствах под воздействием акустических волн.

- Разведка побочных электромагнитных излучений и наводок электронных средств обработки информации (ПЭМИН), обеспечивающая добывание информации, содержащейся непосредственно в формируемых, передаваемых или отображаемых (телефонных и факсимильных) сообщениях и документах с использованием радиоэлектронной аппаратуры, регистрирующей непреднамеренные прямые электромагнитные излучения и электрические сигналы средств обработки информации, а также вторичные электромагнитные излучения и электрические сигналы, наводимые прямыми электромагнитными излучениями в токопроводящих цепях различных технических устройств и токопроводящих элементах конструкций зданий и сооружений.
- Телевизионная, фотографическая и визуальная оптическая разведка, обеспечивающая добывание информации, содержащейся в изображениях объектов, получаемых в видимом диапазоне электромагнитных волн с использованием телевизионной аппаратуры.

Угрозы несанкционированного доступа

- «Маскарад» (присвоение идентификатора пользователя), использование чужих пользовательских идентификаторов, раскрытие паролей и другой аутентификационной информации.
- Несанкционированный доступ (НСД) к ресурсам ЛВС компании со стороны внутренних злоумышленников.
- НСД к ресурсам ЛВС компании со стороны внешних

- злоумышленников.
- НДС к журналам аудита.
 - НДС к средствам аудита.
 - Внешний нарушитель может выдавать себя за легального пользователя путем подделывания адресов в заголовках сетевых пакетов либо информации канального уровня.
 - Сбои в работе средств защиты могут предоставить возможность реализации попытки НДС для потенциального нарушителя (переход в небезопасное состояние). Кроме того, при восстановлении системы безопасное состояние может быть восстановлено некорректно либо может быть утеряна часть данных аудита.
 - НДС к веб-сайту компании и внешним хостам со стороны внешних злоумышленников.
 - НДС к беспроводной сети компании.
 - НДС к резервным копиям данных.
 - Использование внутренними и внешними нарушителями уязвимых мест в компонентах системы защиты. Нарушители могут случайно или в результате целенаправленного поиска обнаружить уязвимые места в средствах защиты, которыми можно воспользоваться для получения НДС к информации.
 - Использование ошибок проектирования, кодирования либо конфигурации ПО.
 - Анализ и модификация ПО.
 - Использование недеklarированных возможностей в ПО, оставленных для отладки либо умышленно внедренных.
 - Внедрение несанкционированного, непроверенного или вредоносного программного кода (вирусов, троянских программ и т.п.).
 - Логические бомбы, пересылаемые по e-mail.

Угрозы недоступности ИТ сервисов и разрушения (утраты) информационных

АКТИВОВ

- Атаки на отказ в обслуживании против внешних хостов компании.
- Недоступность ИТ сервисов и информации по причине физического или логического сбоя компьютерного или периферийного оборудования (например, электричество, водоснабжение, отопление, вентиляция, кондиционирование и т.п.).
- Сбой системы кондиционирования воздуха.
- Запыление.
- Повреждение носителей информации.
- Сбой сетевого оборудования.
- Флуктуации в сети электропитания.
- Установка непроверенных технических средств или замена вышедших из строя аппаратных компонент на неидентичные компоненты.
- Недоступность внешних ИТ ресурсов и информации по причине технического сбоя в каналах связи.
- Сбой коммуникационных сервисов.
- Физическое повреждение сетевого и каналобразующего оборудования внутренними нарушителями.
- Физическое повреждение линий связи внешними или внутренними нарушителями.
- Разрушение данных по причине системного сбоя или ошибки ПО, использование непротестированного ПО.
- Внедрение несанкционированного или непротестированного кода.
- Сбой в системах безопасности.
- Внесение случайных или непреднамеренных изменений в программное обеспечение и средства совместного использования данных в вычислительной среде.
- Неумышленное разрушение критичной для бизнеса информации (файлов данных, программ, баз данных, конфигурационной информации и т.п.) со стороны инсайдеров.
- Ущерб, наносимый тестами на проникновение.

- Потеря (уничтожение) записей.
- Нарушение безопасности по причине несоблюдения операционных процедур.
- Нарушение безопасности по причине неточных, неполных или неподходящих планов обеспечения непрерывности, недостаточного тестирования или несвоевременного обновления планов.
- Умышленное разрушение критичной для бизнеса информации (файлов данных, программ, баз данных, конфигурационной информации и т.п.) со стороны инсайдеров.
- Умышленное разрушение критичной для бизнеса информации (файлов данных, программ, баз данных, конфигурационной информации и т.п.) со стороны внешних злоумышленников.
- Уничтожение планов обеспечения непрерывности бизнеса.
- Умышленная порча ПО и резервных копий внутренними нарушителями.
- Воздействие на технические или программные средства в целях нарушения целостности (уничтожения, искажения) информации, работоспособности технических средств, средств защиты информации, адресности и своевременности информационного обмена (электромагнитное, через специально внедренные электронные и программные средства («закладки»).

Угрозы нарушения целостности и несанкционированной модификации данных

- Нарушение целостности данных из-за ошибок пользователей.
- Нарушение целостности систем и данных, неумышленная модификация системной конфигурации, файлов данных, баз данных, отчетов и т.п. в результате ошибок технического персонала.
- Ошибка в процессах сопровождения.

- Ошибка персонала технической поддержки.
- Изменение конфигурации активного сетевого оборудования.
- Нарушение целостности систем или данных, несанкционированное изменение системной конфигурации, файлов данных, баз данных, отчетов и т.п. со стороны инсайдеров.
- Фальсификация записей.
- Мошенничество.
- Несанкционированная модификация журналов аудита.
- Несанкционированная или непреднамеренная модификация.

Угрозы антропогенных и природных катастроф

- Антропогенные катастрофы (взрыв, терроризм, вандализм, другие способы умышленного причинения ущерба).
- Бомбардировка.
- Забастовка.
- Природные катастрофы (затопление, пожар, ураган, землетрясение и т.п.).
- Молния.
- Ураган.

Юридические угрозы

- Нарушение прав интеллектуальной собственности.
- Нелегальное использование программного обеспечения.
- Несанкционированное использование информационных материалов, являющихся интеллектуальной собственностью.
- Нарушение патентного права.
- Нарушение (несоответствие требованиям) законодательства и нормативной базы.
- Нелегальный импорт/экспорт программного обеспечения.

- Невыполнение контрактных обязательств.