Приложение 6. Перечень типовых уязвимостей информационной безопасности

написано Александр Астахов | 11 июня, 2023

Следующие перечни содержат примеры уязвимостей в различных областях безопасности, включая примеры угроз, которые могут использовать эти уязвимости. Эти перечни могут пригодиться при оценке уязвимостей.

Безопасность кадровых ресурсов (ISO/IEC 27002:2005, раздел 8)

Уязвимость	Угроза, использующая уязвимость
Недостаточное обучение безопасности	Ошибка персонала технической поддержки
Неосведомленность в вопросах безопасности	Ошибки пользователей
Отсутствие механизмов мониторинга	Несанкционированное использование программного обеспечения
Отсутствие политик в области корректного использования средств телекоммуникаций и передачи сообщений	Несанкционированное использование сетевого оборудования
Не отменяются права доступа при увольнении	Несанкционированный доступ
Не существует процедуры, гарантирующей возврат ресурсов при увольнении	Кража
Немотивированный или недовольный персонал	Злоупотребление средствами обработки информации

Уязвимость	Угроза, использующая уязвимость
Безнадзорная работа внешнего персонала или персонала, работающего в нерабочее время	Кража

Физическая безопасность и безопасность окружающей среды (ISO/IEC 27002:2005, раздел 9)

Уязвимость	Угроза, использующая уязвимость
Неадекватное или небрежное использование механизмов физического контроля доступа в здание, комнаты и офисы	Умышленное причинение вреда
Отсутствие физической защиты здания, дверей и окон	Кража
Размещение в зоне, подверженной затоплению	Затопление
Незащищенное хранение	Кража
Недостаточное сопровождение/неудачная установка средств хранения информации	Ошибка в процессе сопровождения
Отсутствие схемы периодической замены оборудования	Износ средств хранения информации
Подверженность оборудования влажности, пыли и загрязнению	Запыление
Подверженность оборудования перепадам температур	Нарушение температурного режима
Подверженность оборудования колебаниям напряжения	Флуктуация электропитания
Нестабильное электропитание	Флуктуация электропитания

Управление коммуникациями и операциями (ISO/IEC 27002:2005, раздел 10)

Уязвимость	Угроза, использующая уязвимость
Сложный пользовательский интерфейс	Ошибка персонала
Передача или повторное использование средств хранения информации без надлежащей очистки	Несанкционированный доступ к информации
Неадекватный контроль изменений	Сбой системы безопасности
Неадекватное управление сетью	Перегрузка трафика
Отсутствие процедур резервного копирования	Потеря информации
Отсутствие доказательств отправки или получения сообщения	Уход от ответственности
Отсутствие обновления программного обеспечения, используемого для защиты от вредоносного кода	Вирусная инфекция
Нет разделения обязанностей	Злоупотребление системой (случайное или преднамеренное)
Нет разделения тестового и рабочего оборудования	Несанкционированная модификация действующих систем
Неконтролируемое копирование	Кража
Незащищенные соединения с сетями общего пользования	Использование программного обеспечения неавторизованными пользователями

Контроль доступа (ISO/IEC 27002:2005, раздел 11)

Уязвимость	Угроза, использующая уязвимость
Неправильное разграничение доступа в сетях	Несанкционированные подключения к сетям
Отсутствие политик чистых столов и чистых экранов	Потеря или повреждение информации
Отсутствие механизмов идентификации и аутентификации, таких как аутентификация пользователей	Присвоение чужого пользовательского идентификатора
Отсутствие защиты мобильного компьютерного оборудования	Несанкционированный доступ к информации
Отсутствующая или некорректная политика контроля доступа	Несанкционированный доступ к информации, системам или программному обеспечению
Отсутствие «выхода из системы», когда покидается рабочая станция	Использование программного обеспечения неавторизованными пользователями
Отсутствие или проведение в недостаточном объеме тестирования программного обеспечения	Использование программного обеспечения неавторизованными пользователями
Отсутствие контроля и анализа прав доступа пользователей	Доступ со стороны пользователей, покинувших организацию или сменивших место работы
Плохое управление паролями (легко угадываемые пароли, хранение паролей, недостаточно частая смена)	Присвоение чужого пользовательского идентификатора
Отсутствие отключения и изменения стандартных предустановленных учетных записей и паролей	Несанкционированный доступ к информации, системам и программному обеспечению

Уязвимость	Угроза, использующая уязвимость
Неконтролируемое использование системных утилит	Обход механизмов контроля системы или приложения

Приобретение, разработка и сопровождение информационных систем (ISO/IEC 27002:2005, раздел 12)

Уязвимость	Угроза, использующая уязвимость
Недостаточная защита криптографических ключей	Раскрытие информации
Несовершенная политика в области использования криптографии	Нарушение законодательства или нормативной базы
Отсутствие контроля входных или выходных данных	ошибка
Отсутствие проверки обрабатываемых данных	Искажение информации
Невыполнение или выполнение в недостаточном объеме тестирования программного обеспечения	Использование программного обеспечения неавторизованными пользователями
Плохо документированное программное обеспечение	Ошибка персонала технической поддержки
Непонятные или неполные спецификации для разработчиков	Сбой программного обеспечения
Неконтролируемая загрузка и использование программного обеспечения	Вредоносное программное обеспечение

Уязвимость	Угроза, использующая уязвимость
Неконтролируемое использование условно бесплатного или бесплатного программного обеспечения в корпоративных приложениях	Юридическая ответственность
Хорошо известные дефекты в программном обеспечении	Использование программного обеспечения неавторизованными пользователями
Неправильный выбор тестовых данных	Несанкционированный доступ к персональным данным