

НИУ МЭИ

Отчет по лабораторной работе №1

Группа: ТФ-13-22

Бригада: 2

Студенты: Дубишкин Д.Д.

Мартиросян М.Д.

Лобанов П.В.

Маркаров М.Г.

Филаков А.С.

Жаркова А.Э.

Аннотация:

"Компания future-perfect design оказывает услуги 3d сканирования объектов любых размеров, в том числе лазерное 3д сканирование зданий, сооружений и местности. Обратный инжиниринг и BIM - моделирование. Создание планов и чертежей. Выпуск конструкторской документации."

Термины и сокращения:

Информационная система: совокупность содержащейся в базах данных информации и обеспечивающих ее обработку информационных технологий и технических средств

Угроза безопасности информации (УБИ): совокупность условий и факторов, создающих потенциальную или реально существующую опасность нарушения безопасности информации.

Уязвимость: недостаток (слабость) программного (программно-технического) средства или информационной системы в целом, который (которая) может быть использована для реализации угроз безопасности информации.

Задачи:

Определить 5 информационных объектов и найти для каждого 3-4 угрозы
Составить граф связей угроза-объект
Предложить варианты защиты

1) Хранилище САД моделей

УБИ 006 - Угроза внедрения кода или данных

Защита: резервное копирование данных

УБИ 015 - Угроза доступа к защищаемым файлам с использованием обходного пути

Защита: правильная настройка доступа к защищаемым файлам

УБИ 091 - Угроза несанкционированного удаления защищаемой информации

Защита: резервное копирование данных

УБИ 089 - Угроза несанкционированного редактирования реестра

Защита: правильная настройка доступа к реестру

2) База данных клиентов

УБИ 026 - Угроза искажения XML-схемы

Защита: шифровка сетевого трафика между клиентом и сервером

УБИ 088 - Угроза несанкционированного копирования защищаемой информации

Защита: правильная настройка доступа к защищаемой информации, работа с персоналом

УБИ 023 - Угроза изменения компонентов информационной (автоматизированной) системы

Защита: работа с персоналом, невозможность доступа к этим компонентам из вне

УБИ 102 - Угроза опосредованного управления группой программ через совместно используемые данные

Защита: надежный механизм контроля внесенных изменений

3) Архив ВІМ данных

УБИ 124 - Угроза подделки записей журнала регистрации событий

Защита: защищенный формат записей, работа с персоналом

УБИ 093 - Угроза несанкционированного управления буфером

Защита: надежный механизм проверки ввода данных

УБИ 020 - Угроза злоупотребления возможностями, предоставленными потребителям облачных услуг

Защита: правильная настройка интерфейса

УБИ 122 - Угроза повышения привилегий

Защита: ручное управление привилегиями пользователей

4) База данных геометрии объектов клиентов

УБИ 090 - Угроза несанкционированного создания учётной записи пользователя

Защита: ручное управление учетными записями пользователей

УБИ 077 - Угроза несанкционированного доступа к данным за пределами резервированного адресного пространства, в том числе выделенного под виртуальное аппаратное обеспечение

Защита: файрвол, вайтлист

УБИ 102 - Угроза опосредованного управления группой программ через совместно используемые данные

Защита: надежный механизм контроля внесенных изменений

5) Архив пользовательских файлов

УБИ 175 - Угроза «фишинга»

Защита: научить персонал компании не переходить по непонятным ссылкам

УБИ 177 - Угроза неподтверждённого ввода данных оператором в систему, связанную с безопасностью

Защита: работа с персоналом, надежная система проверки ввода

УБИ 100 - Угроза обхода некорректно настроенных механизмов аутентификации

Защита: механизм проверки параметров аутентификации

УБИ 132 - Угроза получения предварительной информации об объекте защиты

Защита: мониторинг подозрительных запросов из вне



