**Основы информационной безопасности**

**Задание 1. База данных угроз**

**Выполнил**: Селуянов Данила Дмитриевич, гр. 932102

**Результат выполнения работы**

**1. Список определений терминов**Угроза – совокупность условий и факторов, создающих опасность нарушения информационной безопасности

Уязвимость – слабые места информационного актива или средства контроля и управления, которые могут быть использованы злоумышленниками.

Конфиденциальность – свойство информации, указывающее на необходимость введения ограничений на круг субъектов, имеющих доступ к данной информации

Целостность – свойство информации существовать в неискажаемом виде

Доступность – возможность своевременного беспрепятственного доступа к информации

**2. Список изученных угроз и уязвимостей**

**Изученные угрозы:**

**УБИ. 076**   
Угроза несанкционированного доступа к гипервизору из виртуальной машины и (или) физической сети

**Описание угрозы**Угроза заключается в возможности приведения нарушителем всей (если гипервизор – один) или части (если используется несколько взаимодействующих между собой гипервизоров) виртуальной инфраструктуры в состояние «отказ в обслуживании» путём осуществления деструктивного программного воздействия на гипервизор из запущенных в созданной им виртуальной среде виртуальных машин, или осуществления воздействия на гипервизор через его подключение к физической вычислительной сети.  
Данная угроза обусловлена наличием множества разнообразных интерфейсов взаимодействия между гипервизором и виртуальной машиной и (или) физической сетью, уязвимостями гипервизора, а также уязвимостями программных средств и ограниченностью функциональных возможностей аппаратных средств, используемых для обеспечения его работоспособности.  
Реализация данной угрозы возможна в одном из следующих случаев:  
наличие у нарушителя привилегий, достаточных для осуществления деструктивного программного воздействия из виртуальных машин;  
наличие у гипервизора активного интерфейса взаимодействия с физической вычислительной сетью

**Источник угрозы**Внутренний нарушитель со средним потенциалом, внешний нарушитель со средним потенциалом

**Объект воздействия** Гипервизор

**Последствия реализации угрозы** Нарушение доступности

**УБИ. 078**  
Угроза несанкционированного доступа к защищаемым виртуальным машинам из виртуальной и (или) физической сети

**Описание угрозы**Угроза заключается в возможности осуществления нарушителем деструктивного программного воздействия на виртуальные машины из виртуальной и (или) физической сети как с помощью стандартных (не виртуальных) сетевых технологий, так и с помощью сетевых технологий виртуализации.  
Данная угроза обусловлена наличием у создаваемых виртуальных машин сетевых адресов и возможностью осуществления ими сетевого взаимодействия с другими субъектами.  
Реализация данной угрозы возможна при условии наличия у нарушителя сведений о сетевом адресе виртуальной машины, а также текущей активности виртуальной машины на момент осуществления нарушителем деструктивного программного воздействия

**Источник угрозы**Внутренний нарушитель с низким потенциалом, внешний нарушитель с низким потенциалом

**Объект воздействия** Виртуальная машина

**Последствия реализации угрозы**  
Нарушение конфиденциальности, нарушение целостности, нарушение доступности

**УБИ. 079**  
Угроза несанкционированного доступа к защищаемым виртуальным машинам со стороны других виртуальных машин

**Описание угрозы**Угроза заключается в возможности осуществления деструктивного программного воздействия на защищаемые виртуальные машины со стороны других виртуальных машин с помощью различных механизмов обмена данными между виртуальными машинами, реализуемых гипервизором и активированных в системе.  
Данная угроза обусловлена слабостями механизма обмена данными между виртуальными машинами и уязвимостями его реализации в конкретном гипервизоре.  
Реализация данной угрозы возможна при условии наличия у нарушителя привилегий, достаточных для использования различных механизмов обмена данными между виртуальными машинами, реализованных в гипервизоре и активированных в системе

**Источник угрозы**Внутренний нарушитель с низким потенциалом, внешний нарушитель с низким потенциалом

**Объект воздействия** Виртуальная машина

**Последствия реализации угрозы**  
Нарушение конфиденциальности, нарушение целостности, нарушение доступности

**Изученные уязвимости:**

**BDU:2022-03386**Уязвимость набора инструментов для веб-разработки DevTools браузеров Microsoft Edge и Google Chrome, позволяющая нарушителю раскрыть защищаемую информацию

**Описание уязвимости** Уязвимость набора инструментов для веб-разработки DevTools браузеров Microsoft Edge и Google Chrome связана с чтением за границами буфера в памяти. Эксплуатация уязвимости может позволить нарушителю, действующему удалённо, раскрыть защищаемую информацию с помощью специально созданной веб-страницы

**Тип ошибки** Чтение за границами буфера

**Класс уязвимости** Уязвимость кода

**Способ устранения** Обновление программного обеспечения

**BDU:2022-03347**Уязвимость компонента Performance Manager браузера Google Chrome, позволяющая нарушителю выполнить произвольный код

**Описание уязвимости** Уязвимость компонента Performance Manager браузера Google Chrome связана с использованием памяти после её освобождения. Эксплуатация уязвимости может позволить нарушителю, действующему удалённо, выполнить произвольный код с помощью специально созданной веб-страницы

**Тип ошибки** Использование после освобождения

**Класс уязвимости** Уязвимость кода

**Способ устранения** Обновление программного обеспечения

**BDU:2022-00074**  
Уязвимость набора инструментов для веб-разработки DevTools браузера Google Chrome, позволяющие нарушителю обойти существующие ограничения безопасности с помощью специально созданной HTML страницы

**Описание уязвимости**Уязвимость набора инструментов для веб-разработки DevTools браузера Google Chrome связана с ошибками шифрования данных. Эксплуатация уязвимости может позволить нарушителю, действующему удаленно, обойти существующие ограничения безопасности с помощью специально созданной HTML страницы

**Тип ошибки** Проблемы использования криптографии

**Класс уязвимости** Уязвимость кода

**Способ устранения** Обновление программного обеспечения