МИНИСТЕРСТВО НАУКИ И ВЫСШЕГО ОБРАЗОВАНИЯ РОССИЙСКОЙ ФЕДЕРАЦИИ

Федеральное государственное автономное образовательное учреждение высшего профессионального образования «СЕВЕРО-КАВКАЗСКИЙ ФЕДЕРАЛЬНЫЙ УНИВЕРСИТЕТ» Институт сервиса, туризма и дизайна (филиал) СКФУ в г. Пятигорске

Методические указания по выполнению практических работ по дисциплине «Персональная кибербезопасность»

СОДЕРЖАНИЕ

1. ЦЕЛЬ И ЗАДАЧИ ОСВОЕНИЯ ДИСЦИПЛИНЫ

Цель изучения дисциплины « Профессиональная кибербезопасность » подготовка студента к решению внештатных ситуаций касательной дестабилизации информационной системы или нарушения целостности данных, а также их потери.

2. НАИМЕНОВАНИЕ ПРАКТИЧЕСКИХ РАБОТ

№ темы	Наименование тем практических работ	Объем часов (астр)	Интерактивная форма проведения
Тема 1. Введение в кибербезопасность			
1	Первичные навыки обеспечения кибербезопасности на рабочем месте	3	
Тема 3. Классификация угроз в информационных системах			
3	Анализ разрушительности кибератак	3	
3	Приоритизация классов киберугроз	3	
Тема 4. Анализ способов борьбы с фишингом			
4	Основные способы выявления фишинг атак	1,5	Компьютерные симуляции
Тема 5. Выявление и устранение возможности организации социальной инженерии в профессиональной деятельности			
5	Моделирование поведения злоумышленника в момент проведения социальной инженерии	1,5	
	Итого	12	3

3. СОДЕРЖАНИЕ ПРАКТИЧЕСКИХ РАБОТ

Практическая работа № 1. Первичные навыки обеспечения кибербезопасности на рабочем месте.

Форма проведения: практическая работа.
Содержание: *получение навыков работы по организации безопасного рабочего места*
Задачи практической работы:

1. Первичный анализ автоматизированного рабочего места.
2. Поиск участков информационной системы с некорректно установленным уровнем доступа.

Используемые инструменты: Одной из основных задач любого сотрудника имеющего индивидуальное автоматизированное рабочее место – это умение проводить первичный анализ на предмет выявления возможного проведения кибератак.

Понятие: Кибератака – это п окушение на информационную безопасность компьютерной системы.

Вводный курс: первичный анализ подразумевает под собой осмотр рабочего места с целью определения существующей схемы организации информационной безопасности . Исходя из этого, проведите детальный анализ ус тановленных программных комплексов обеспечивающих безопасность вашей операционной системы. Полученные результаты зарисуйте в виде схемы, в которой необходимо ввести понятия внутренней системы безопасности и внешней. Следовательно, при зарисовке схемы все П О которое установленное для анализа файловой системы, реестра и т.д. необходимо представить внутри прямоугольника. Таким образом, прямоугольник будет отражать границы вашей ОС. Все комплексы, которые нацелены на решение задач по предотвращению внешних угроз, следует представить за границами прямоугольника. Также, следует отметить, что обязательным являются пометки внешней защиты такими маркерами как «исходящая фильтрация», «входящая фильтрация». Представленный вариант показать преподавателю.

Задачи для самостоятельного решения

1. Определите участки операционной системы в которой некорректно установлены права доступа т.е., пользователь может вносить корректировки в те участки в которых он не должен имеет пара доступа.

Работа с литературой:

Рекомендуемые источники информации (№ источника)			
Основная	Дополнительная	Методическая	Интернет-ресурсы
1-2	1-2	1-2	1

Оценочные средства: отчет к практической работе (См.: Фонд оценочных средств)

Практическая работа № 2 Анализ разрушительности кибератак.

Форма проведения: практическая работа

Содержание: изучение негативных последствий в условиях успешно организованных кибератака.

Ход практической работы:

Задачи практической работы:

1. Ознакомиться с возможными кибератаками;

2. Ознакомиться с результатами успешно реализованных кибератак;
3. Анализ последствий кибератак;
4. Выполнить самостоятельное задание.

Используемые инструменты : поиск и анализ существующих кибератак в глобальной сети возможно провести лишь посредством использования поисковых служ б. Таким образом, для организации поиска значений кибератак потребуется воспользоваться поисковой системой Google или Yandex.

Понятие: Анализ - это метод исследования, характеризующийся выделением и изучением отдельных частей объектов исследования.

Поисковая система - это компьютерная система, предназначенная для поиска информации. Одно из наиболее известных применений поисковых систем - веб-сервисы для поиска текстовой или графической информации во Всемирной паутине.

Вводный курс: Поисковая служба Google имеет огромный список инструментов для поиска информации. В основной массе запросов пользователи используют лишь стандартный инструмент – это поле ввода без дополнительных параметров, однако, использование дополнений позволит сократить полученные результа ты от поисковой службы от нескольких тысяч до нескольких десятков страниц, в которых будет лишь актуальная информация. При условии поиска статьи или страницы с определенным заголовком который отображается во вкладке следует использовать следующие параметры:

Allintitle:"текст для поиска" – поиск всех введенных слов в заголовках

Intitle:"текст для поиска" – поиск только абсолютного совпадения в заголовках

Осуществление поиска информации возможно также регулировать по географической принадлежности или классификации. Как известно все сайты доступны посредством доменных имен, а каждое доменное имя имеет свою зону которая относится к стране. Таким образом, если необходимо осуществить поиск информации только в рунете, тогда следует обратиться к доменной зон е RU. Пример выглядит следующим образом:

```
Текст поиска site:ru
```

Если необходимо произвести поиск только на государственных площадках РФ, тогда запрос будет выглядеть:

```
Текст поиска site:gov.ru
```

Следовательно на образовательных площадках:

```
Текст поиска site:edu.ru
```

Также поиск можно осуществлять непосредственно в рамках одного сайта. Таким образом:

```
Расписание site:pf.ncfu.ru
```

При условии необходимости поиска определенной фразы с абсолютным совпадением, следует, взять данную фразу в кавычки:

```
“Фраза которую необходимо найти”
```

Необходимость поиска файла с определенным расширением реализуется посредством следующей команды:

```
Filetype: расширение
```

Следовательно, если необходимо найти документ в формате *.doc с заголовком «Киберугрозы» запрос будет выглядеть следующим образом:

```
Киберугрозы Filetype:doc
```

Полный список операторов представлен в таблице 1.

Таблица 1 – Операторы поисковой системы Google

Оператор	**Назначение**
AND	Поиск 1-го, 2-го и N-го слова (логическое «И», используется по умолчанию)
OR	Поиск 1-го или 2-го слова (логическое «ИЛИ»)
“”	Поиск точной фразы, заключенной в “”
+	Выделение главных ключевых слов в запросе
–	Исключение нежелательных слов в результатах поисковой выдачи
site:	Поиск по конкретному сайту
related:	Поиск похожих страниц (обычно этот оператор применяется для поиска

Оператор	Назначение
	похожих сайтов)
link:	Поиск ссылающихся страниц
~	Включение в выдачу синонимов выделенного слова
filetype:	Поиск документов по расширению
define:	Поиск определений
cache:	Обращение к странице, сохраненной в кеше поисковой машины
allinurl:	Поиск страниц, содержащих в своем адресе все слова из поискового запроса
inurl:	Поиск страниц, содержащих в своем адресе слова из поискового запроса в любом порядке и в любом количестве
inanchor:	Поиск в тексте ссылок
allintitle:	Поиск страниц, содержащих в своем заголовке все слова из поискового запроса
intitle:	Поиск страниц, содержащих в своем заголовке слова из поискового запроса в любом порядке и в любом количестве
allintext:	Поиск страниц, содержащих все слова поискового запроса
:	Задает регион поиска
info:	Показывает информацию о странице
.	Соответствует символу «пробела» в составных запросах

Задачи для самостоятельного решения

1. Используя выше представленные инструменты поиска, самостоятельно найти киберугрозы для персонального компьютера работающего как рабочая станция в организации.

Работа с литературой:

Рекомендуемые источники информации (№ источника)

Основная	Дополнительная	Методическая	Интернет-ресурсы
1-3	1-2	1-3	1-4

Оценочные средства: отчет к пратической работе (См.: Фонд оценочных средств)

Практическая работа № 3 Приоритизация классов киберугроз.

Форма проведения: практическая работа
Содержание: *классификация киберугроз*
Ход практической работы:

Задачи практической работы:

1. Ознакомиться с классами киберугроз;
2. Выполнить самостоятельное задание.

Используемые инструменты : командный интерпретатор CMD операционной системы Windows.

Понятие: Cmd — это интерпретатор командной строки для операционных систем Windows В операционных системах семейства Windows NT для архитектуры IA -32 и OS/2 имеется и COMMAND.COM для совместимости со старыми программами. В настройках интерпретатора присутствует возможность изменить размер курсора, шрифт, цвет текста и размер окна.

Вводный курс: киберугрозы можно классифицировать по признаку управления: «сетевые» и « локальные». Под класс локальных попадают различные вирусы которыми может быть заражен компьютер. Сетевые атаки предполагают использование злоумышленником специального п рограммного обеспечения, которое посредством установленного соединения на зараженном устройстве позволяет им управлять.

Обеспечение безопасности устройства обеспечивается антивирусом, однако, инфицирование может быть произведено в момент нулевого дня. Под нулевым днем подразумевается момент выпуска вредоносного ПО в глобальную сеть. В данный момент в антивирусных базах отсутствует код данного вируса и пользовательская система на период обновления базы является уязвимой. Стандартными средствами операционной системы возможно в некоторых случаях определить был ли заражен компьютер. Данную возможность, возможно, реализовать посредством командной строки.

В первую очередь следует обратить внимание на характерные признаки поведения вредоносного ПО. Касательно локал ьных угроз принцип строится на использовании вычислительных ресурсов устройства, следовательно, необходимо проанализировать

нагрузку. Сетевые угрозы создают дополнительные подключения, которые также можно проследить. Для этого следует запустить командную строку.

Для запуска данного интерпретатора следует нажать на кнопку «Пуск» и в поле поиск ввести «cmd.exe», затем нажать кнопку «Enter», после чего откроется окно интерпретатора, как представлено на рисунке 1.

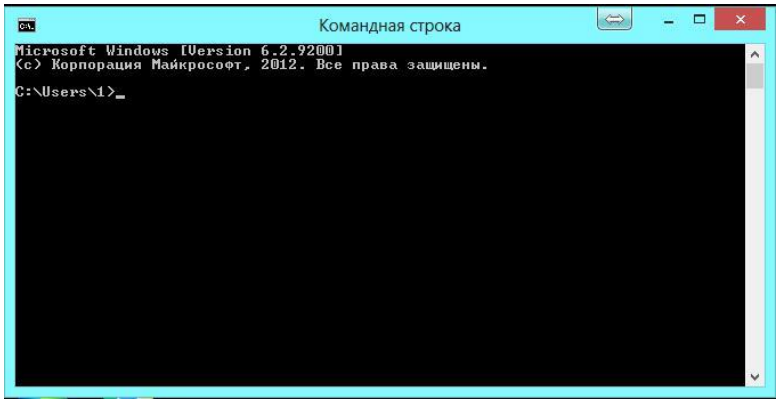

Рисунок 1 – Окно командной строки CMD.EXE

Для получения списка команд используемых в данном интерпретаторе, следует, ввести команду help и нажать клавишу Enter после чего в окне отобразится список. Для отображения нагрузки оказываемое на вычислительную машину, необходимо отобразить список запущенн ых приложений. Для решения данной задачи, следует выполнить команду tasklist. Пример выполнения команды представлен на рисунке 2.

```
C:\Users\1>tasklist

Имя образа                     PID Имя сессии          № сеанса       Память
========================= ======== ================ =========== ============
System Idle Process              0 Services                   0         20 КБ
System                           4 Services                   0     24 028 КБ
smss.exe                       348 Services                   0      1 024 КБ
csrss.exe                      528 Services                   0      4 312 КБ
wininit.exe                    620 Services                   0      3 704 КБ
csrss.exe                      636 Console                    1     16 048 КБ
winlogon.exe                   684 Console                    1      7 996 КБ
services.exe                   724 Services                   0     10 708 КБ
lsass.exe                      732 Services                   0     14 276 КБ
svchost.exe                    832 Services                   0      9 872 КБ
svchost.exe                    884 Services                   0     12 060 КБ
atiesrxx.exe                   944 Services                   0      4 488 КБ
svchost.exe                    976 Services                   0     23 612 КБ
dwm.exe                       1004 Console                    1     36 876 КБ
svchost.exe                    552 Services                   0    331 844 КБ
svchost.exe                    372 Services                   0     12 304 КБ
atieclxx.exe                  1052 Console                    1      7 788 КБ
```

Рисунок 2 – Результат выполнения команды tasklist

Как видно из рисунка 2, результат команды отображается в 5 столбцах:

- имя образа – название запущенной программы;
- PID – уникальный номер запущенного приложения выданный операционной системой;
- имя сессии – тип выделенной сессии ОС для работы программы;
- № сеанса – определяет номер класса сессии;
- память – отображает занимаемое пространство оперативной памяти программой.

Деление на данные столбцы необходимо для возможности фильтрации отображаемых процессов. К примеру можно отсортировать по номеру сеанса все запущенные приложения. Узнать синтаксис программы возможно посредством использования команды help. Пример выглядит следующим образом: help tasklist.

Используя полученные данные о параметрах команды отобразим запущенные программы которые работают в сессии console.

Tasklist /FI “SESSION eq 1”

Параметр eq представляет оператор рав енства. Полный список операторов представлен ниже:

- EQ – равно;
- NE - не равно;
- LT – меньше;
- LE - меньше или равно;
- GT – больше;
- GE - больше или равно.

Данная команда необходимо для анализа запущенных программ. Используя полученный список с установленными фильтрами, можно отследить запущенные программы которые вызывают некоторое сомнение. Такого рода программы необходимо проверить. Для этого копируете название программ ы и вводите в поисковой запрос, после чего получаете информацию о данном приложении. Если в процессе поиска определится вредоносность данного ПО, тогда немедленно завершите процесс посредством команды taskkill /PID номер приложения. После завершения процесса необходимо найти и удалить данный файл, в первую очередь необходимо обновить антивирусн ые базы, после чего выполнить полную проверку компьютера на предмет поиска вирусов. Если вредоносное

ПО не обнаружено, самостоятельно посредством поиска по названию файла отправьте его на карантин.

Для выявления сетевых угроз, необходимо отследить динамику открытых соединений посредством команды netstat. Полный перечень параметров можно получить вызвав команду следующим образом netstat /? .

Как видно из списка параметров есть возможность фильтрации вывода идентификатора приложения которое установило соедин ение, отображение используемого файла программы. Таким образом составим команду для вывода списка программ с установленными сетевыми соединениями.

netstat –b –o

В результате получим список представленный на рисунке 3.

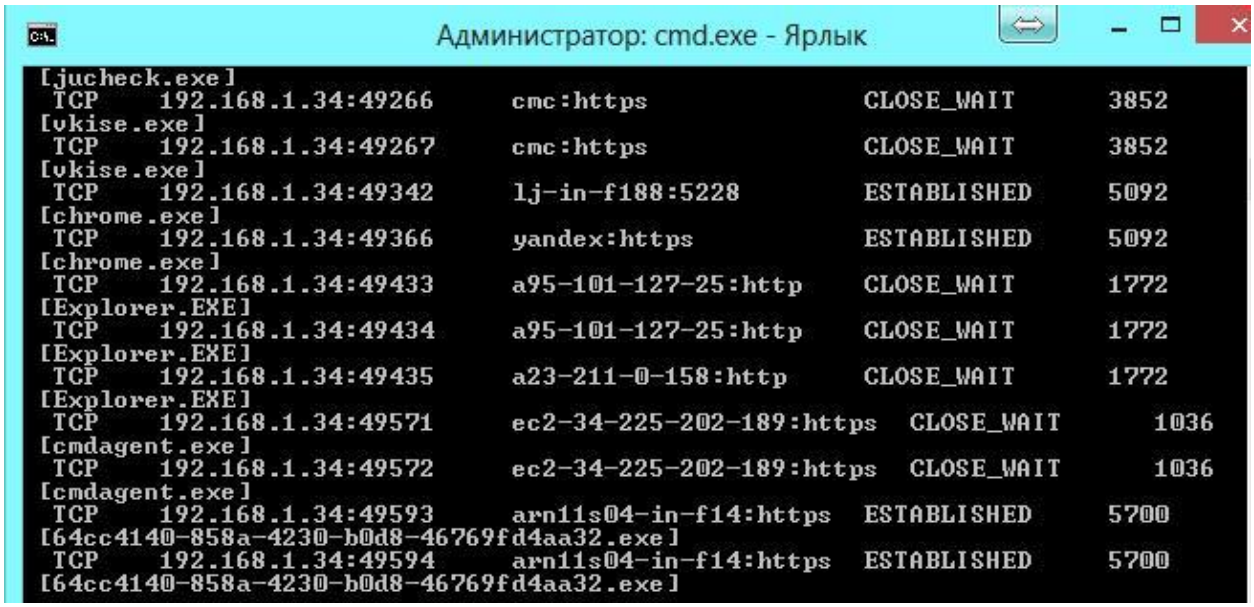

Рисунок 3 – результат сетевой статистики

Как видно в последних строках присутствуют два активных соединения, которые запущены программой с подозрительным именем. Следовательно, используя полученные имена подозрительных программ, производим поиск посредством поисковых сервисов и при условии подтверждения вредоносности данного ПО, производим процедуру, которая была описана выше, по очищению вирусов.

Задачи для самостоятельного решения

1.Провести анализ своего ПК и результат представить в отчете с подробным описанием каждого процесса.

Работа с литературой:

Рекомендуемые источники информации (№ источника)			
Основная	Дополнительная	Методическая	Интернет-ресурсы
1-3	1-2	1-3	1-4

Оценочные средства: отчет к пратической работе (См.: Фонд оценочных средств).

Практическая работа № 4. Основные способы выявления фишинг атак.

Форма проведения: *практическая работа*

Содержание: получение навыков работы по выявлению фишинг атак.

Ход практической работы:

Задачи практической работы:

1. Получить навыки выявления фишинг атак.

Используемые инструменты: поисковая система.

Понятие: Фишиг — вид интернет -мошенничества, целью которого является получение доступа к конфиденциальным данным пользователей — логинам и паролям. Это достигается путём проведения массовых рассылок электронных писем от имени популярных брендов, а также личных сообщений внутри различных сервисов, например, от имени банков или внутри социальных сетей. В письме часто содержится прямая ссылка на сайт, внешне неотличимый от настоящего, либо на сайт с редиректом. После того как пользователь попадает на поддельную страницу, мошенники пытаются различными психологическими приёмами побудить пользователя ввести на поддельной странице свои логин и пароль, которые он использует для доступа к определённому сайту, что позволяет мошенникам получить доступ к аккаунтам и банковским счетам.

Задачи для самостоятельного решения

1. Используя полученные навыки работы с поисковой системой, определить наиболее актуальные методы фишинг атак и представить их в отчете.

Работа с литературой:

Рекомендуемые источники информации (№ источника)			
Основная	Дополнительная	Методическая	Интернет-ресурсы

1-3	1-2	1-3	1-4

Оценочные средства: отчет к пратической работе (См.: Фонд оценочных средств).

Практическая работа № 5. Моделирование поведения злоумышленника в момент проведения социальной инженерии

Форма проведения: *практическая работа*

Содержание: *Изучение основы социальной инженерии.*

Ход практической работы:

Задачи практической работы:

1. Изучить основные социальной инженерии;
2. Освоить методы противостояния социальной инженерии.

Используемые инструменты: Социальная инженерия — совокупность приёмов, методов и технологий создания такого пространства, условий и обстоятельств, которые максимально эффективно приводят к конкретному необходимому результату, с использованием социологии и психологии. Для России это явление достаточно новое, оно ранее рассматривалась как метод управления действиями человека без использования технических средств, который основан на использовании слабостей человеческого фактора и считается очень разрушительны м. Зачастую социальную инженерию рассматривают как незаконный метод получения информации, однако это не совсем так. Если рассматривать современную профессиональную социальную инженерию, то область её применения вполне законна - например, она помогает дости чь изначально недостижимый результат, или "программировать" для совершения позитивных и полезных действий конкретного человека. Конечно, сегодня социальную инженерию зачастую используют в интернете для получения закрытой информации или информации, которая представляет большую ценность.

Для того, чтобы обезопасить себя от воздействия социальной инженерии, необходимо понять, как она работает. Рассмотрим основные типы социальной инженерии и методы защиты от них.

Претекстинг - это набор действий, отработанных по определенному, заранее составленному сценарию, в результате которого жертва может выдать какую -либо информацию или совершить определенное действие. Чаще всего данный вид атаки предполагает использование голосовых средств, таких как Skype, телефон и т.п.

Для использования этой техники злоумышленнику необходимо изначально иметь некоторые данные о жертве (имя сотрудника; должность; название проектов, с которыми

он работает; дату рождения). Злоумышленник изначально использует реальные запросы с именем сотрудников компании и, после того как войдет в доверие, получает необходимую ему информацию.

Фишинг – техника интернет -мошенничества, направленная на получение конфиденциальной информации пользователей - авторизационных данных различных систем. Основным видом ф ишинговых атак является поддельное письмо, отправленное жертве по электронной почте, которое выглядит как официальное письмо от платежной системы или банка. В письме содержится форма для ввода персональных данных (пин - кодов, логина и пароля и т.п) или ссыл ка на web-страницу, где располагается такая форма. Причины доверия жертвы подобным страницам могут быть разные: блокировка аккаунта, поломка в системе, утеря данных и прочее.

Троянский конь – это техника основывается на любопытстве, страхе или других эмоциях пользователей. Злоумышленник отправляет письмо жертве посредством электронной почты, во вложении которого находится «обновление» антивируса, ключ к денежному выигрышу или компромат на сотрудника. На самом же деле во вложении находится вредоносная програ мма, которая после того, как пользователь запустит ее на своем компьютере, будет использоваться для сбора или изменение информации злоумышленником.

Кви про кво (услуга за услугу) – данная техника предполагает обращение злоумышленника к пользователю по элек тронной почте или корпоративному телефону. Злоумышленник может представиться, например, сотрудником технической поддержки и информировать о возникновении технических проблем на рабочем месте. Далее он сообщает о необходимости их устранения. В процессе «реш ения» такой проблемы, злоумышленник подталкивает жертву на совершение действий, позволяющих атакующему выполнить определенные команды или установить необходимое программное обеспечение на компьютере жертвы.

Дорожное яблоко – этот метод представляет собой а даптацию троянского коня и состоит в использовании физических носителей (CD, флэш -накопителей). Злоумышленник обычно подбрасывает такой носитель в общедоступных местах на территории компании (парковки, столовые, рабочие места сотрудников, туалеты). Для того, чтобы у сотрудника возник интерес к данному носителю, злоумышленник может нанести на носитель логотип компании и какую -нибудь подпись. Например, «данные о продажах», «зарплата сотрудников», «отчет в налоговую» и другое.

Обратная социальная инженерия - данный вид атаки направлен на создание такой ситуации, при которой жертва вынуждена будет сама обратится к злоумышленнику за «помощью». Например, злоумышленник может выслать письмо с телефонами и контактами «службы поддержки» и через некоторое время создать обратимые неполадки в компьютере жертвы. Пользователь в таком случае позвонит или свяжется по электронной почте с злоумышленником сам, и в процессе «исправления» проблемы злоумышленник сможет получить необходимые ему данные.

Задачи для самостоятельного решения

1. Используя поисковые службы составить отчет об актуальных методах защиты от социальной инженерии.

Работа с литературой:

Рекомендуемые источники информации (№ источника)			
Основная	Дополнительная	Методическая	Интернет-ресурсы
1-3	1-2	1-3	1-4

4. МЕТОДИЧЕСКИЕ МАТЕРИАЛЫ, ОПРЕДЕЛЯЮЩИЕ ПРОЦЕДУРЫ ОЦЕНИВАНИЯ ЗНАНИЙ, УМЕНИЙ, НАВЫКОВ, ХАРАКТЕРИЗУЮЩИХ ЭТАПЫ ФОРМИРОВАНИЯ КОМПЕТЕНЦИЙ

Текущая аттестация студентов проводится преподавателем, ведущим практические занятия по дисциплине « Профессиональная кибербезо пасность» в форме собеседования, выполнения индивидуальных заданий. Допуск к лабораторным работам происходит при наличии у студентов печатного варианта отчета. Защита отчета проходит в форме устного ответа студента по выполненной работе и ответов на вопро сы преподавателя. При оценивании ответа студентов учитывается полнота и степень раскрытия темы, владение материалом, ответов на дополнительные вопросы.

Максимальное количество баллов студент получает, если он активно участвует в работе, владеет материалом, умеет логично и четко излагать мысли, творчески подходит к решению основных вопросов темы, показывает самостоятельность мышления.

Основанием для снижением оценки являются:

- слабое знание темы и основной терминологии;
- пассивность участия в групповой работе;
- отсутствие умения применить теоретические знания для решения практических задач;
- несвоевременность предоставления выполненных работ.

5. УЧЕБНО-МЕТОДИЧЕСКОЕ И ИНФОРМАЦИОННОЕ ОБЕСПЕЧЕНИЕ ДИСЦИПЛИНЫ

Учебно-методическое и информационное обеспечение дисциплины	
Основная литература	1. Старостина, Е. В. Защита от компьютерных преступлений и кибертерроризма : вопросы и ответы / Е.В. Старостина, Д.Б. Фролов. - М. : Эксмо, 2005. - 192 с.

	2. Словарь-справочник терминов в области кибербезопасности : [около 2000 терминов] / М -во образования и науки Рос. Федерации, Федер. гос. автоном. науч. учреждение "Центр информационных технологий и систем органов исполнительной власти" ; [авт.-сост.: И.М. Во ронков, А. В. Дроздов, С. В. Петров и др.] ; [рук. проекта А. В. Старовойтов]. - Москва : Сам полиграфист, 2014. - 229 с.
Дополнительная литература	1. Курушин, В. Д. Компьютерные преступления и информационная безопасность : Справочник. - М. : Новый Юрист, 1998. - 256с. 2. Кевин Митник, Вильям Саймон Искусство вторжения: ДМК пресс, Компания АйТи, 2005. – 337с.
Методическая литература	1. Методические указания по выполнению практических работ по дисциплине Профессиональная кибербезопасность; 2. Методические рекомендации для студентов по организации самостоятельной работы по дисциплине Профессиональная кибербезопасность.
Интернет-ресурсы	1. Современные уязвимости программного обеспечения [Электронный ресурс] / https://www.securitylab.ru/vulnerability/ Обновляемые списки вредоносного ПО [Электронный ресурс] : https://www.securitylab.ru/virus/
Программное обеспечение	Последние версии популярных WEB браузеров; Антивирусные приложения; Сканеры портов.
Материально-техническое обеспечение	Учебныеаудитории, оборудованные учебной мебелью, интерактивной доской, персональными компьютерами, мультимедийным проектором для проведения лекционных и практических занятий.