Министерство науки и высшего образования Российской Федерации
Федеральное государственное бюджетное образовательное учреждение
высшего образования
«Вятский государственный университет»

УТВЕРЖДАЮ
Начальник управления дополнительного образования и международной деятельности
_____ / Ю. С. Топорова
«02» апреля 2021
рег. № 03-04-2021-0424-0714

**Рабочая программа**
**учебной дисциплины (модуля)**
«Основы кибербезопасности и киберугроз для противодействия преступлениям с использованием информационно-коммуникационных технологий»

дополнительной профессиональной программы –
программы повышения квалификации
«Основы кибербезопасности и киберугроз для противодействия преступлениям с использованием информационно-коммуникационных технологий»

Киров, 2021

Рабочая программа составлена в соответствии с требованиями дополнительной профессиональной программы «Основы кибербезопасности и киберугроз для противодействия преступлениям с использованием информационно-коммуникационных технологий»

Рабочая программа разработана:
Частиков Александр Вениаминович, профессор, д-р техн. наук
*(Ф.И.О., должность, уч. степень разработчика)*

## 1. Рабочая учебная программа

### 1.1 Пояснительная записка

Актуальность и значение учебной дисциплины «Основы кибербезопасности и киберугроз для противодействия преступлениям с использованием информационно-коммуникационных технологий» определяются тем, что в настоящее время практически во всех отраслях и сферах деятельности применяются компьютерные и информационно-коммуникационные системы. Злоумышленники, используя уязвимости этих систем, могут реализовывать различные киберугозы. Специалистам в области информационной безопасности необходимо грамотно использовать и настраивать методы защиты, тем самым препятствуя кибератакам.

**Цели и задачи учебной дисциплины**

| | |
|---|---|
| Цель учебной дисциплины | Получение компетенций в вопросах кибербезопасности и защиты от киберугроз |
| Задачи учебной дисциплины | Дать представление об основных видах уязвимостей современных компьютерных систем.<br>Проанализировать наиболее актуальные киберугрозы.<br>Познакомить с криптографическими и программно-аппаратными средствами защиты информации.<br>Получить практические навыки работы с методами защиты от существующих киберугроз.<br>Развить навыки самостоятельной работы с различными источниками по вопросам информационной безопасности. |

**Компетенции слушателя, формируемые в результате освоения учебной дисциплины / модуля**

В результате освоения учебной дисциплины (модуля) обучающийся должен демонстрировать следующие результаты образования

| Виды деятельности | Профессиональные компетенции | Практический опыт | Умения | Знания |
|---|---|---|---|---|
| 62.09 Деятельность, связанная с | ПК 1 Способен осуществлять расследование инцидентов в области информационной безопасности с использованием | Анализировать вредоносное ПО, работать с криптографией, оцени- | Анализировать защищенность информационно- | Наиболее распространенные виды киберугроз, механизм |

| | | | | |
|---|---|---|---|---|
| использованием вычислительной техники и информационных технологий | информационно-коммуникационных технологий | вать состояние защищенности информационных систем. | коммуникационных средств, проводить аудит безопасности, разрабатывать рекомендации по противодействию киберугрозам. | кибербезопасности, методы защиты персонального компьютера и мобильных устройств. |

## 1.2 Содержание учебной дисциплины (модуля)

## Объем учебной дисциплины и виды учебной работы

| Форма обучения | Общий объем (трудоемкость) Часов | в том числе аудиторная контактная работа обучающихся с преподавателем, час | | | | | Самостоятельная работа, час | Форма промежуточной аттестации |
|---|---|---|---|---|---|---|---|---|
| | | Всего | Лекции | Практические (семинарские) занятия | Лабораторные занятия | Консультации | | |
| очная | 48 | 36 | 24 | 12 | | | 12 | Зачет |

## Тематический план

| № п/п | Основные разделы и темы учебной дисциплины | Часы | | Самостоятельная работа |
|---|---|---|---|---|
| | | Лекции | практические (семинарские занятия) | |
| 1. | Уязвимости современных компьютерных систем | 2 | 2 | 1 |
| 2. | Основы криптографии | 2 | 2 | 1 |
| 3. | Методы проверки подлинности | 2 | | 1 |
| 4. | Системы обнаружения вторжений | 2 | | 1 |
| 5. | Межсетевое экранирование | 2 | 2 | 1 |
| 6. | Виртуальные частные сети | 2 | | 1 |
| 7. | Анализ защищенности | 2 | 2 | 1 |
| 8. | Антивирусные средства защиты информации | 2 | 2 | 1 |
| 9. | Системы предотвращения утечек информации | 2 | | 1 |
| 10. | Виртуализация информационных систем | 2 | 2 | 1 |
| 11 | Безопасное восстановление информационных систем | 2 | | 1 |
| 12 | Управление информационной инфраструктурой | 2 | | 1 |
| | Итого: | 24 | 12 | 12 |

**Матрица соотнесения разделов / тем учебной дисциплины / модуля и формируемых в них компетенций**

| *Разделы / темы учебной дисциплины* | *Количество часов* | *Компетенции* |
|---|---|---|
| | | ПК-1 |
| Уязвимости современных компьютерных систем | *5* | V |
| Основы криптографии | *5* | V |
| Методы проверки подлинности | *3* | V |
| Системы обнаружения вторжений | *3* | V |
| Межсетевое экранирование | *5* | V |
| Виртуальные частные сети | *3* | V |
| Анализ защищенности | *5* | V |
| Антивирусные средства защиты информации | *5* | V |
| Системы предотвращения утечек информации | *3* | V |
| Виртуализация информационных систем | *5* | V |
| Безопасное восстановление информационных систем | *3* | V |
| Управление информационной инфраструктурой | *3* | V |
| *Итого* | *48* | |

**Краткое содержание учебной дисциплины:**

**Тема 1.** Уязвимости современных компьютерных систем

В данном разделе слушатель познакомится с основными понятиями информационной безопасности: угрозы, уязвимости, атаки. Будут рассмотрены особенности современных киберсистем и кибератак.

Кроме того, слушатель получит возможность проследить во времени основные этапы развития методов и средств защиты компьютерной информации.

**Тема 2.** Основы криптографии

В данной теме будут рассмотрены основные методы защиты информации на основе криптографических преобразований данных: шифрование - способ обеспечения секретности данных, контроль целостности - проверка неизменности данных, неотказуемость - проверка авторства.

**Тема 3.** Методы проверки подлинности

В данном разделе слушатель познакомится с основными этапами, которые должен пройти пользователь, прежде чем получить доступ к информационным ресурсам: идентификация, аутентификация, авторизация. Будут рассмотрены методы проверки подлинности пользователей от простых паролей до сложных биометрических систем. Не останутся без внимания и методы проверки подлинности информационной системы при дистанционном доступе к ней.

**Тема 4.** Системы обнаружения вторжений

В данном разделе слушатели познакомятся со средствами автоматического реагирования на выявленные кибератаки, а также методами сбора и анализа информации на основе которых они функционируют. Будут рассмотрены особенности функционирования различных видов подобных систем.

**Тема 5.** Межсетевое экранирование

В данном разделе слушатели познакомятся с принципами и технологиями ограничения информационных потоков на границе между безопасной внутренней частью и потенциально враждебной внешней частью информационной системы. В числе прочих будут рассмотрены и персональные межсетевые экраны, которые защищают от внешних угроз только один компьютер или любое другое устройство.

**Тема 6.** Виртуальные частные сети

В данном разделе будет рассмотрены технологии обеспечения защищенного взаимодействия между отдельными компьютерами или сегментами корпоративной информационной системы через недоверенное информационное пространство, например, через Интернет или сеть провайдера, где любые переданные данные могут быть перехвачены или искажены злоумышленником

**Тема 7.** Анализ защищенности

В данном разделе будут рассмотрены этапы проведения мероприятий по проверке информационных систем на наличие в них уязвимостей, а также методы и средства автоматического поиска уязвимостей. Такие средства могут быть использованы как для проведения атаки на систему, так и для своевременного устранения обнаруженных недостатков.

**Тема 8.** Антивирусные средства защиты информации

В данном разделе будет дана классификация вредоносных компьютерных программ, будут рассмотрены различные методы их обнаружения, а также состав и принципы работы антивирусных средств.

**Тема 9.** Системы предотвращения утечек информации

Системы предотвращения утечек информации - единственный класс средств защиты информации, который позволяет выявлять превышение полномочий разрешенными пользователями. В данной теме слушатели узнают о принципах работы подобных систем, основных каналах утечки информации и методах их обнаружения.

**Тема 10.** Виртуализация информационных систем

В данном разделе слушатели познакомятся с технологией виртуализации - представлением "физического" компьютера или сервера в виде программного образа, позволяющим сделать информационную инфраструктуру более управляемой и экономичной. Также будут рассмотрены угрозы информационной безопасности, связанные с использованием виртуальных систем.

**Тема 11.** Безопасное восстановление информационных систем

Современные информационные системы должны продолжать обслуживание пользователей даже в случае возникновения неисправностей. В данной теме будут рассмотрены основные подходы, которые применяются для обеспечения

бесперебойной работы информационной системы, а также методы выявления и устранения неисправностей без прерывания ее работы.

**Тема 12.** Управление информационной инфраструктурой

Функционирование информационной системы крупной организации невозможно без централизованной системы управления, которая в автоматическом режиме собирает информацию о состоянии каждого компьютера или другого устройства и управляет их программным обеспечением. В данном разделе слушатель познакомится с видами, особенностями построения и функционирования таких систем.

## 2. Учебно-методическое обеспечение дисциплины

### 2.1. Методические рекомендации для преподавателя

Организация учебного процесса предусматривает применение инновационных форм учебных занятий, развивающих у обучающихся навыки командной работы, межличностной коммуникации, принятия решений, лидерские качества (включая, при необходимости, проведение интерактивных лекций, групповых дискуссий, ролевых игр, тренингов, анализ ситуаций и имитационных моделей, в том числе с учетом региональных особенностей профессиональной деятельности выпускников и потребностей работодателей).

### 2.2. Методические указания для слушателей

Успешное освоение учебной дисциплины предполагает активное, творческое участие обучающегося на всех этапах ее освоения путем планомерной, повседневной работы. Обучающийся обязан посещать лекции и семинарские (практические, лабораторные) занятия, получать консультации преподавателя и выполнять самостоятельную работу.

Выбор методов и средств обучения, образовательных технологий осуществляется преподавателем исходя из необходимости достижения обучающимися планируемых результатов освоения дисциплины, а также с учетом индивидуальных возможностей обучающихся из числа инвалидов и лиц с ограниченными возможностями здоровья.

Изучение дисциплины следует начинать с проработки настоящей рабочей программы, методических указаний и разработок, указанных в программе, особое внимание уделить целям, задачам, структуре и содержанию дисциплины.

Главной задачей каждой лекции является раскрытие сущности темы и анализ ее основных положений. Содержание лекций определяется настоящей рабочей программой дисциплины.

Лекции – это систематическое устное изложение учебного материала. На них обучающийся получает основной объем информации по каждой конкретной теме. Лекции обычно носят проблемный характер и нацелены на

освещение наиболее трудных и дискуссионных вопросов, кроме того они способствуют формированию у обучающихся навыков самостоятельной работы с научной литературой.

Предполагается, что обучающиеся приходят на лекции, предварительно проработав соответствующий учебный материал по источникам, рекомендуемым программой. Часто обучающимся трудно разобраться с дискуссионными вопросами, дать однозначный ответ. Преподаватель, сравнивая различные точки зрения, излагает свой взгляд и нацеливает их на дальнейшие исследования и поиск научных решений. После лекции желательно вечером перечитать и закрепить полученную информацию, тогда эффективность ее усвоения значительно возрастает. При работе с конспектом лекции необходимо отметить материал, который вызывает затруднения для понимания, попытаться найти ответы на затруднительные вопросы, используя предлагаемую литературу. Если самостоятельно не удалось разобраться в материале, сформулируйте вопросы и обратитесь за помощью к преподавателю.

Целью практических и лабораторных занятий является проверка уровня понимания обучающимися вопросов, рассмотренных на лекциях и в учебной литературе, степени и качества усвоения материала; применение теоретических знаний в реальной практике решения задач; восполнение пробелов в пройденной теоретической части курса и оказания помощи в его освоении.

Практические (лабораторные) занятия в равной мере направлены на совершенствование индивидуальных навыков решения теоретических и прикладных задач, выработку навыков интеллектуальной работы, а также ведения дискуссий. Конкретные пропорции разных видов работы в группе, а также способы их оценки определяются преподавателем, ведущим занятия.

На практических (лабораторных) занятиях под руководством преподавателя обучающиеся обсуждают дискуссионные вопросы, отвечают на вопросы тестов, закрепляя приобретенные знания, выполняют практические (лабораторные) задания и т.п. Для успешного проведения практического (лабораторного) занятия обучающемуся следует тщательно подготовиться.

Основной формой подготовки обучающихся к практическим (лабораторным) занятиям является самостоятельная работа с учебно-методическими материалами, научной литературой, статистическими данными и.т.п.

Изучив конкретную тему, обучающийся может определить, насколько хорошо он в ней разобрался. Если какие-то моменты остались непонятными, целесообразно составить список вопросов и на занятии задать их преподавателю. Практические (лабораторные) занятия предоставляют студенту возможность творчески раскрыться, проявить инициативу и развить навыки публичного ведения дискуссий и общения, сформировать определенные навыки и умения и т.п.

Самостоятельная работа слушателей включает в себя выполнение различного рода заданий (изучение учебной и научной литературы, материалов лекций, систематизацию прочитанного материала, подготовку контрольной работы, решение задач и т.п.), которые ориентированы на более глубокое

усвоение материала изучаемой дисциплины. По каждой теме учебной дисциплины преподаватель предлагает обучающимся перечень заданий для самостоятельной работы. Самостоятельная работа по учебной дисциплине может осуществляться в различных формах (например: подготовка докладов; написание рефератов; публикация тезисов; научных статей; подготовка и защита проекта; другие).

К выполнению заданий для самостоятельной работы предъявляются следующие требования: задания должны исполняться самостоятельно либо группой и представляться в установленный срок, а также соответствовать установленным требованиям по оформлению.

Регулярно рекомендуется отводить время для повторения пройденного материала, проверяя свои знания, умения и навыки по контрольным вопросам.

Результатом самостоятельной работы должно стать формирование у обучающегося определенных знаний, умений, навыков, компетенций.

При проведении промежуточной аттестации обучающегося учитываются результаты текущей аттестации в течение периода обучения.

Процедура оценивания результатов освоения учебной дисциплины (модуля) осуществляется на основе действующего Положения об организации текущего контроля успеваемости и промежуточной аттестации обучающихся ВятГУ.

Для приобретения требуемых компетенций, хороших знаний и высокой оценки по дисциплине обучающимся необходимо выполнять все виды работ своевременно в течение всего периода обучения.

## 3. Учебно-методическое обеспечение учебной дисциплины

### Основная литература

1. Программно-аппаратные средства обеспечения информационной безопасности : учебное пособие для вузов / А.В. Душкин, О.М. Барсуков, К.В. Славнов, Е.В. Кравцов. - Москва : Горячая линия - Телеком, 2016. - 248 с. : схем., табл., ил. - Библиогр.: с. 234-235. - ISBN 978-5-9912-0470-5 : Б. ц. - URL: http://biblioclub.ru/index.php?page=book&id=483768/ (дата обращения: 24.03.2020). - Режим доступа: ЭБС Университетская библиотека ONLINE. - Текст : электронный.

2. Хорев, Павел Борисович. Программно-аппаратная защита информации : учеб. пособие / П. Б. Хорев. - Москва : Форум, 2013. - 351 с. - Библиогр.: с. 347-349. - ISBN 978-5-91134-353-8 (в пер.) : 401.00 р. - Текст : непосредственный.

и т.д.

3. Платонов, Владимир Владимирович. Программно-аппаратные средства защиты информации : учебник / В. В. Платонов. - Москва : Академия, 2013. - 330, [1] с. - (Высшее профессиональное образование. Бакалавриат. Информационная безопасность). - Библиогр.: с. 326-327. - ISBN 978-5-7695-9327-7 : 579.70 р. - Текст : непосредственный.

4. Богульская, Н. А. Модели безопасности компьютерных систем : учебное пособие / Н. А. Богульская, М. М. Кучеров. - Красноярск : СФУ, 2019. - 206 с. - ISBN 978-5-7638-4008-7 : Б. ц. - URL: https://e.lanbook.com/book/157578 (дата обращения: 15.05.2020). - Режим доступа: ЭБС Лань. - Текст : электронный.

5. Криптографические методы защиты информации. - Санкт-Петербург : ПГУПС, 2018 - . - Текст : электронный.Ч. 2. - Санкт-Петербург : ПГУПС, 2018. - 63 с. - ISBN 978-5-7641-1215-2 : Б. ц. - URL: https://e.lanbook.com/book/138103 (дата обращения: 15.05.2020). - Режим доступа: ЭБС Лань.

### Дополнительная литература

1. Фомин, Д. В. Информационная безопасность и защита информации: специализированные аттестованные программные и программно-аппаратные средства / Д. В. Фомин. - Благовещенск : АмГУ, 2017. - 240 с. - Б. ц. - URL: https://e.lanbook.com/book/156494 (дата обращения: 15.05.2020). - Режим доступа: ЭБС Лань. - Текст : электронный.

2. Проскурин, В. Г. Защита в операционных системах : учебное пособие для вузов / В.Г. Проскурин. - Москва : Горячая линия - Телеком, 2014. - 192 с. - ISBN 978-5-9912-0379-1 : Б. ц. - URL: http://biblioclub.ru/index.php?page=book&id=275128/ (дата обращения: 24.03.2020). - Режим доступа: ЭБС Университетская библиотека ONLINE. - Текст : электронный.

3. Проскурин, Вадим Геннадьевич. Защита программ и данных : учеб. пособие / В. Г. Проскурин. - 2-е изд., стер. - Москва : Академия, 2012. - 198, [1] с. - (Высшее профессиональное образование. Бакалавриат. Информационная безопасность). - Библиогр.: с.195-196. - ISBN 978-5-7695-9288-1 : 495.00 р. - Текст : непосредственный.

4. Загинайлов, Ю. Н. Теория информационной безопасности и методология защиты информации : учебное пособие / Ю.Н. Загинайлов. - М.|Берлин : Директ-Медиа, 2015. - 253 с. - ISBN 978-5-4475-3946-7 : Б. ц. - URL:

http://biblioclub.ru/index.php?page=book&id=276557/ (дата обращения: 24.03.2020). - Режим доступа: ЭБС Университетская библиотека ONLINE. - Текст : электронный.

5. Вычислительные системы и компьютерные сети. - Майкоп : АГУ. - Текст : электронный.Ч. 1 : Вычислительные системы и компьютерные сети. - Майкоп : АГУ, 2018. - 80 с. - ISBN 978-5-85108-328-0 : Б. ц. - URL: https://e.lanbook.com/book/146133 (дата обращения: 15.05.2020). - Режим доступа: ЭБС Лань.

6. Кирпичников, А. П. Криптографические методы защиты компьютерной информации : учебное пособие / А.П. Кирпичников, З.М. Хайбуллина. - Казань : Казанский научно-исследовательский технологический университет (КНИТУ), 2016. - 100 с. : табл., схем. - Библиогр. в кн. - ISBN 978-5-7882-2052-9 : Б. ц. - URL: http://biblioclub.ru/index.php?page=book&id=560536/ (дата обращения: 24.03.2020). - Режим доступа: ЭБС Университетская библиотека ONLINE. - Текст : электронный.

7. Игнатьев, Е. Б. Основы криптографии : учебное пособие / Е. Б. Игнатьев. - Иваново : ИГЭУ, 2020. - 88 с. - Б. ц. - URL: https://e.lanbook.com/book/154559 (дата обращения: 15.05.2020). - Режим доступа: ЭБС Лань. - Текст : электронный.

## Перечень ресурсов информационно-телекоммуникационной сети «Интернет», необходимых для освоения дисциплины

1. Портал дистанционного обучения ВятГУ.
2. Раздел официального сайта ВятГУ, содержащий описание образовательной программы.

## Описание материально-технической базы, необходимой для осуществления образовательного процесса

### Перечень специализированных аудиторий (лабораторий)

| Вид занятий | Назначение аудитории |
|---|---|
| *Практика, лекция* | *Учебная аудитория.* |
| *Самостоятельная работа* | *Читальные залы библиотеки* |
| | |

### Перечень специализированного оборудования

| Перечень используемого оборудования |
|---|
| *МУЛЬТИМЕДИА-ПРОЕКТОР С ЭКРАНОМ НАСТЕННЫМ* |
| *НОУТБУК (ПЕРСОНАЛЬНЫЙ КОМПЬЮТЕР)* |

## Перечень информационных технологий, используемых при осуществлении образовательного процесса по учебной дисциплине

| № п. п | Наименование ПО | Краткая характеристика назначения ПО | Производитель ПО и/или поставщик ПО |
|---|---|---|---|

| | | | |
|---|---|---|---|
| 1 | Программная система с модулями для обнаружения текстовых заимствований в учебных и научных работах «Антиплагиат.ВУЗ» | Программный комплекс для проверки текстов на предмет заимствования из Интернет-источников, в коллекции диссертация и авторефератов Российской государственной библиотеки (РГБ) и коллекции нормативно-правовой документации LEXPRO | ЗАО "Анти-Плагиат" |
| 2 | Microsoft Office 365 Student Advantage | Набор веб-сервисов, предоставляющий доступ к различным программам и услугам на основе платформы Microsoft Office, электронной почте бизнес-класса, функционалу для общения и управления документами | ООО "Рубикон" |
| 3 | Office Professional Plus 2013 Russian OLP NL Academic. | Пакет приложений для работы с различными типами документов: текстами, электронными таблицами, базами данных, презентациями | ООО "СофтЛайн" (Москва) |
| 4 | Windows 7 Professional and Professional K | Операционная система | ООО "Рубикон" |
| 5 | Kaspersky Endpoint Security длябизнеса | Антивирусное программное обеспечение | ООО «Рубикон» |
| 6 | Информационная система КонсультантПлюс | Справочно-правовая система по законодательству Российской Федерации | ООО «КонсультантКиров» |
| 7 | Электронный периодический справочник «Система ГАРАНТ» | Справочно-правовая система по законодательству Российской Федерации | ООО «Гарант-Сервис» |
| 8 | Security Essentials (Защитник Windows) | Защита в режиме реального времени от шпионского программного обеспечения, вирусов. | Microsoft |

## 4. Материалы, устанавливающие содержание текущего контроля успеваемости (ТКУ) и самостоятельной работы слушателей

*Формы ТКУ:*

– собеседование;
– тест;

*Формы самостоятельной работы:*

– конспектирование;
– реферирование литературы;
– аннотирование книг, статей;
– выполнение заданий поисково-исследовательского характера;
– углубленный анализ научно-методической литературы;
– работа с лекционным материалом: проработка конспекта лекций, работа на полях конспекта с терминами, дополнение конспекта материалами из рекомендованной литературы;
– участие в работе семинара: подготовка сообщений, докладов, заданий;

## 5. Материалы, устанавливающие содержание и порядок проведения промежуточных аттестаций

К сдаче зачета допускаются все слушатели, проходящие обучение на данной ДПП, вне зависимости от результатов текущего контроля успеваемости и посещаемости занятий, при этом, результаты текущего контроля успеваемости могут быть использованы преподавателем при оценке уровня усвоения обучающимися знаний, приобретения умений, навыков и сформированности компетенций в результате изучения учебной дисциплины.

Промежуточная аттестация проводится в форме зачета (тестовых заданий).

Зачет принимается преподавателями, проводившими лекции по данной учебной дисциплине.

## Методические рекомендации по подготовке и проведению промежуточной аттестации

Промежуточная аттестация проводится в целях повышения эффективности обучения, определения уровня профессиональной подготовки обучающихся и контролем за обеспечением выполнения стандартов обучения.

## Перечень примерных тестовых вопросов к зачету

На что направлены атаки DoS?

1. **Атаки DoS нацелены на нарушение работы сети путем истощения доступной полосы пропускания.**
2. Атаки DoS нацелены на нарушение работы сети путем ограничения авторизации пользователей.
3. Атаки DoS нацелены на нарушение работы сети путем отключения активного оборудования.
4. Механические повреждения.

Что представляет собой виртуальная частная сеть VPN?

1. **Виртуальная частная сеть VPN (Virtual Private Network,) является общим понятием, описывающим любое сочетание технологий для безопасного соединения но незащищенным или ненадежным сетям.**
2. Виртуальная частная сеть VPN (Virtual Private Network,) является общим понятием, описывающим любое сочетание технологий для общедоступного соединения но незащищенным или ненадежным сетям.
3. Виртуальная частная сеть VPN (Virtual Private Network,) является понятием, описывающим особое сочетание технологий для безопасного соединения по защищенным или надежным сетям.
4. Виртуальная частная сеть VPN (Virtual Private Network,) является общим понятием, описывающим любое сочетание технологий для безопасного соединения по сетям общего пользования.

Какой тип атак нацелен на нарушение работы сети путем истощения доступной полосы пропускания.

1. **Атака DoS.**
2. Вирусы типа Троянский конь.
3. Сканирование адресов.
4. Подделка IP адреса хоста.

Каковы цели управления учетными записями?

1. **Измерять параметры использования сети, чтобы можно было соответствующим образом описывать отдельных пользователей или их группы.**
2. Измерять параметры использования сети, чтобы можно было соответствующим образом описывать отдельных пользователей или их группы.
3. Измерять параметры сети, чтобы можно было соответствующим образом регулировать доступ пользователей или их групп.
4. Измерять описания, чтобы можно было соответствующим образом регулировать работу в сети активного оборудования.

Какой опасный тип угроз может быть внедрен в почтовые сообщения?

1. **Вирус или "троянский конь" могут быть внедрены в приложение к сообщению электронной почты. Для ослабления такой угрозы рекомендуется использовать антивирусное программное обеспечение.**
2. DoS атаки.
3. Несанкционированный доступ.
4. Механические повреждения оборудования.

Каковы основные типы атак на сеть?

1. **Несанкционированный доступ, ненадежная аутентификация, пароли, анализаторы пакетов, атаки на уровне приложений, вирусы, черви, "троянские кони", кража IP-адресов и отказ в обслуживании (DoS).**
2. Несанкционированный доступ.
3. Анализаторы пакетов, атаки на уровне приложений, вирусы, черви, "троянские кони", кража IP-адресов и отказ в обслуживании (DoS).
4. Кража IP-адресов и отказ в обслуживании (DoS).

Приведите пример эшелонированного решения проблемы безопасности.

1. **Под эшелонированной защитой сети понимается расширение технологий обеспечения безопасности на всю сеть для защиты от угроз безопасности, которые могут возникнуть в любых точках сети. Одним из возможных решений является использование брандмауэра и установка программного обеспечения IDS для отдельных станций на web-серверах. Брандмауэр защищает Web-сереер от нежелательных потоков данных, а программное обеспечение защищает сервер от поступления на него разрешенных данных.**
2. Под эшелонированной защитой сети понимается расширение технологий обеспечения безопасности на всю сеть для защиты от угроз безопасности, которые могут возникнуть лишь в незащищенных точках сети.
3. Одним из возможных решений является использование антивируса и установка лицензионного программного обеспечения для отдельных станций на web-серверах.
4. Брандмауэр защищает Web-сереер от любых потоков данных, а антивирусное программное обеспечение защищает сервер от поступления на него неразрешенных данных.

Какие уровни защищенности устанавливаются в информационных системах при обработке персональных данных?

1. **Специальные, биометрические, общедоступные, иные.**
2. Специальные, биометрические.
3. Специальные, иные.
4. Специальные, общедоступные.

Что понимается под актуальными угрозами безопасности персональных данных?

1. **Совокупность условий и факторов, создающих актуальную опасность несанкционированного, в том числе случайного, доступа к персональным данным при их обработке в информационной системе, результатом которого могут стать уничтожение, изменение, блокирование, копирование, предоставление, распространение персональных данных, а также иные неправомерные действия.**
2. Отдельные условия и факторы, создающие актуальную опасность несанкционированного, в том числе случайного, доступа к персональным данным при их обработке в ин-

формационной системе, результатом которого могут стать уничтожение, изменение, блокирование, копирование, предоставление, распространение персональных данных, а также иные неправомерные действия.

3. События, создающие актуальную опасность несанкционированного, в том числе случайного, доступа к персональным данным при их обработке в информационной системе, результатом которого могут стать уничтожение, изменение, блокирование, копирование, предоставление, распространение персональных данных, а также иные неправомерные действия.
4. Причины, создающие актуальную опасность несанкционированного, в том числе случайного, доступа к персональным данным при их обработке в информационной системе, результатом которого могут стать уничтожение, изменение, блокирование, копирование, предоставление, распространение персональных данных, а также иные неправомерные действия.

Какой тип атак включает в себя рассылку приложений к сообщениям электронной почты? Каким образом отражается такая атака?

1. **Вирус или "троянский конь" могут быть внедрены в приложение к сообщению электронной почты. Для ослабления такой угрозы рекомендуется использовать антивирусное программное обеспечение.**
2. Вирус или "троянский конь" могут быть внедрены в приложение к сообщению электронной почты. Для ослабления такой угрозы рекомендуется использовать маршрутизаторы.
3. Вирус или "троянский конь" могут быть внедрены в приложение к сообщению электронной почты. Для ослабления такой угрозы рекомендуется использовать коммутаторы.
4. Вирус или "троянский конь" могут быть внедрены в приложение к сообщению электронной почты. Для ослабления такой угрозы рекомендуется использовать активное оборудование CISCO.

Какое средство обеспечения безопасности обнаруживает уязвимые места сетевых устройств?

1. **Сканер сетевой безопасности или средство аудита сетевой безопасности, такое как Nessus, идентифицирует точки уязвимости в сети.**
2. Межсетевой экран.
3. Антивирусная программа.
4. Лицензионная операционная система.

## Перечень примерных вопросов и заданий к зачету

1. Настроить политику безопасности DLP системы.
2. Настроить межсетевой экран.
3. Настроить антивирусное ПО.
4. Настроить политику безопасности ОС.
5. Осуществить виртуализацию системы.
6. Выполнить бэкап данных.
7. Осуществить восстановление удаленных данных с носителя.
8. Выполнить стегоанализ данных.
9. Протестировать ресурс на наличие уязвимостей.
10. Исследовать безопасность wi-fi роутера.