Федеральное государственное бюджетное образовательное учреждение
высшего образования

«Уральский институт Государственной противопожарной службы
Министерства Российской Федерации по делам гражданской обороны,
чрезвычайным ситуациям и ликвидации последствий стихийных бедствий»

# ИНФОРМАЦИОННЫЕ СИСТЕМЫ ЗАЩИТЫ ДАННЫХ
# ОСНОВЫ ЗАЩИТЫ ИНФОРМАЦИИ

**Методические рекомендации по подготовке к зачету**

20.05.01 Пожарная безопасность
20.03.01 Техносферная безопасность



Екатеринбург
2022

**Информационные системы защиты данных. Основы защиты информации** [Текст] : методические рекомендации по подготовке к зачету. Специальность 20.05.01 Пожарная безопасность Направление подготовки 20.03.01 Техносферная безопасность / сост. С. А. Худякова, Л. В. Якупова, А. В. Шпаньков. – Екатеринбург : Уральский институт ГПС МЧС России, 2022. – 16 с.

*Составители:* Худякова С. А., доцент кафедры математики и информатики Уральского института ГПС МЧС России, кандидат педагогических наук, доцент;

Якупова Л. В., преподаватель кафедры математики и информатики Уральского института ГПС МЧС России;

Шпаньков А. В., старший преподаватель кафедры математики и информатики Уральского института ГПС МЧС России.

Методические рекомендации по дисциплине «Информатика» предназначены для курсантов, студентов и слушателей, обучающихся по специальности 20.05.01 Пожарная безопасность и направление подготовки 20.03.01 Техносферная безопасность.

Методические рекомендации рассмотрены и одобрены на заседании кафедры математики и информатики от 09.06.2022 г. протокол № 11.

© Худякова С. А., Якупова Л. В., Шпаньков А. В., 2022
© Уральский институт ГПС МЧС России, 2022©

Содержание

ВВЕДЕНИЕ ..... 4
Глава I. Требования к результатам освоения дисциплины ..... 5
Глава II. Структура дисциплины ..... 6
Глава III. Рекомендации по темам дисциплины ..... 6
§ 1 Теоретические основы информационной безопасности ..... 6
§ 2 Методология защиты информации ..... 7
§ 3 Криптографические способы защиты информации ..... 7
§ 4 Антивирусная защита ..... 8
§ 5. Сетевая безопасность ..... 8
§ 1 Теоретические основы информационной безопасности ..... 9
§ 3 Криптографические способы защиты информации ..... 10
§ 4. Антивирусная защита ..... 10
§ 5. Сетевая безопасность ..... 11
ЛИТЕРАТУРА ..... 13

# ВВЕДЕНИЕ

Методические рекомендации по подготовке к зачету «Информационные системы защиты данных», «Основы защиты данных» предназначены для обучающихся по специальности 20.05.01 Пожарная безопасность и направление подготовки 20.03.01 Техносферная безопасность. Рекомендации составлены в соответствии с требованиями Федерального государственного образовательного стандарта высшего образования по специальности 20.05.01 Пожарная безопасность и направление подготовки 20.03.01 Техносферная безопасность, согласно рабочей (учебной) программе дисциплины «Информационные системы защиты данных», «Основы защиты данных».

Целью освоения учебной дисциплины «Основы защиты информации» является формирование у обучающихся профессиональных компетенций в процессе изучения дисциплины для последующего применения в практической деятельности.

Для достижения данных целей предусматривается решение следующих основных задач:

– систематизация, формализация и расширение знаний по основным положениям защиты информации, криптографии и информационной безопасности;

– изучение методов, средств и инструментов антивирусной защиты, применяемых в сфере информационных технологий и связи;

– дать обучающимся достаточно прочные представления о информационной безопасности, включая аппаратную часть и математическое обеспечение;

– привитие навыков работы с антивирусными пакетами и алгоритмами шифрования и криптографии, архиваторами.

– развитие алгоритмического мышления, интеллектуальных и творческих способностей;

– воспитание чувства ответственности за результаты своего труда.

## Глава I. Требования к результатам освоения дисциплины

В результате освоения дисциплины «Информационные системы защиты данных», «Основы защиты данных» обучающийся должен:

| Результат освоения образовательной программы | Содержание компетенции | Результат обучения по дисциплине |
|---|---|---|
| **Р.О.-4.1** Способность осуществлять планирование, подготовку и организацию деятельности пожарно-спасательного подразделения в различных режимах функционирования | **ПК-13.** Способен осуществлять разработку организационно-управленческой и оперативно-тактической документации в подразделениях пожарной охраны, осуществлять документационное обеспечение повседневной деятельности, в том числе с соблюдением режима секретности и информационной безопасности. | **Знать:** основы защиты информации и программное обеспечение, используемое в подразделениях ГПС для электронного документооборота. **Уметь:** выбирать современные программные средства защиты информации и программное обеспечение, используемое в подразделениях ГПС для электронного документооборота. **Владеть:** навыками применения современных программных средств защиты информации и программное обеспечение, используемое в подразделениях ГПС для электронного документооборота. |

| Результат освоения образовательной программы | Содержание компетенции | Результат обучения по дисциплине |
|---|---|---|
| **РО-5.2** Способность проводить анализ эксплуатации технических средств, пожарной и аварийно-спасательной техники с целью совершенствования её использования | **ПК-3.** Способен моделировать и проектировать организационно-управленческие, технико-технологические системы и процессы, осуществлять их функционирование для решения задач пожарной безопасности, в том числе с применением средств автоматизированного проектирования и автоматизированного управления | **Знать:** основы и принципы проведения анализа различных видов информационных систем защиты данных. **Уметь:** применять методики анализа эксплуатации различных видов информационных систем защиты данных. **Владеть:** навыками разработки технических решений совершенствования, внедрения и практического использования информационных систем защиты данных. |
| **РО-2.2** Способность использовать основы экономических знаний в профессиональной | **ПК-19**. Способен планировать, организовывать и осуществлять комплекс контрольных (надзорных) мероприятий за соблюдением обязательных требований пожарной безопасности и другие | **Знать:** основы нормативного правового регулирования информационных систем защиты данных. **Уметь:** применять законодательство, регулирующее отношения в области |

| | | |
|---|---|---|
| деятельности, демонстрировать навыки правовой культуры | контрольно-надзорные функции, квалификацию правонарушений в области пожарной безопасности с учетом степени риска причинения вреда охраняемым законом ценностям. | информационных систем защиты данных.<br>**Владеть:** навыками проведения правоприменительной деятельности по пресечению нарушений требований использования информационных систем защиты данных. |

## Глава II. Структура дисциплины

Общая трудоемкость дисциплин составляет 3 зачетных единицы, или 108 часов. В таблице представлено распределение тем и форм аттестации по периодам изучения для очной и заочной формам обучения.

**Распределение тем дисциплины «Информационные системы защиты данных», «Основы защиты данных» для очной и заочной формам обучения**

Таблица

| № темы | Наименование тем |
|---|---|
| 6 семестр/4 курс | |
| 1 | Теоретические основы информационной безопасности |
| 2 | Методология защиты информации |
| 3 | Криптографические способы защиты информации |
| 4 | Антивирусная защита |
| 5 | Сетевая безопасность |
| Итоговый контроль – зачет | |

## Глава III. Рекомендации по темам дисциплины

В данном разделе методических рекомендаций приведены вопросы, типовые задания (задачи) по изучаемым темам, которые помогут более качественно подготовиться к различным видам аттестации в соответствии с действующей рабочей программой дисциплины «Информатика».

Зачет по дисциплине «Информатика» может проводиться как в традиционной форме (теоретические вопросы и практические задания (задачи)), так и в форме тестов.

### § 1 Теоретические основы информационной безопасности

1. Понятие информации и информационной безопасности.
2. Информация, сообщения, информационные процессы как объекты информационной безопасности.
3. Обзор защищаемых объектов и систем.
4. Понятие «угроза информации».
5. Понятие «риска информационной безопасности».
6. Примеры преступлений в сфере информации и информационных технологий.
7. Сущность функционирования системы защиты информации.
8. Защита человека от опасной информации и от не

информированности в области информационной безопасности.
9. Целостность, доступность и конфиденциальность информации.
10. Классификация информации по видам тайны и степеням конфиденциальности.
11. Понятия государственной тайны и конфиденциальной информации.
12. Жизненные циклы конфиденциальной информации в процессе ее создания, обработки, передачи.
13. Цели и задачи защиты информации.
14. Основные понятия в области защиты информации.
15. Основные составляющие информационной безопасности.
16. Классификация угроз.
17. Классификация средств защиты информации.
18. Методы и средства организационно-правовой защиты информации.
19. Методы и средства инженерно-технической защиты.
20. Программные и программно-аппаратные методы и средства обеспечения информационной безопасности.
21. Модель интеграции информационной безопасности в основную деятельность организации.
22. Понятие Политики безопасности.

## § 2 Методология защиты информации

1. Анализ существующих методик определения требований к защите информации.
2. Параметры защищаемой информации и оценка факторов, влияющих на требуемый уровень защиты информации.
3. Виды мер и основные принципы защиты информации.
4. Организационная структура системы защиты информации.
5. Законодательные акты в области защиты информации.
6. Российские и международные стандарты, определяющие требования к защите информации.
7. Система сертификации РФ в области защиты информации.
8. Основные правила и документы системы сертификации РФ в области защиты информации

## § 3 Криптографические способы защиты информации

1. Введение в основы современных шифров с симметричным ключом.
2. Модульная арифметика.
3. Сравнения и матрицы.
4. Традиционные шифры с симметричным ключом.
5. Алгебраические структуры.
6. Поля. Усовершенствованный стандарт шифрования (AES — Advanced Encryption Standard).
7. Простые числа. Квадратичное сравнение.
8. Криптографическая система RSA. Криптосистемы.
9. Простые криптосистемы.

10. Шифрование методом замены (подстановки).
11. Одноалфавитная подстановка.
12. Многоалфавитная одноконтурная обыкновенная подстановка. \
13. Таблицы Вижинера.
14. Многоалфавитная одноконтурная монофоническая подстановка.
15. Многоалфавитная многоконтурная подстановка.
16. Шифрование методом перестановки.
17. Простая перестановка.
18. Перестановка, усложненная по таблице.
19. Перестановка, усложненная по маршрутам.
20. Шифрование методом гаммирования.
21. Шифрование с помощью аналитических преобразований. Комбинированные методы шифрования.
22. Стандарты шифрования.
23. Стандарт шифрования данных Data Encryption Standard.
24. Режимы работы алгоритма DES.
25. Алгоритм шифрования данных IDEA.
26. Общая схема алгоритма IDEA

## § 4 Антивирусная защита

1. Общие понятия антивирусной защиты.
2. Уязвимости.
3. Классификация вредоносных программ.
4. Признаки присутствия на компьютере вредоносных программ.
5. Методы защиты от вредоносных программ.
6. Основы работы антивирусных программ: Сигнатурный и эвристический анализ.
7. Тестирование работы антивируса.
8. Классификация антивирусов.
9. Режимы работы антивирусов.
10. Антивирусные комплексы

## § 5. Сетевая безопасность

1. Защита информации в локальных сетях.
2. Основы построения локальной компьютерной сети.
3. Уровни антивирусной защиты.
4. Уровень защиты рабочих станций и сетевых серверов.
5. Уровень защиты почты.
6. Уровень защиты шлюзов.
7. Централизованное управление антивирусной защитой.
8. Логическая сеть.
9. Схема сбора статистики в системе антивирусной защиты.
10. Управление ключами шифрования и безопасность сети.
11. Целостность сообщения и установление подлинности сообщения.
12. Криптографические хэш-функции.

13. Цифровая подпись.
14. Установление подлинности объекта.
15. Управление ключами.
16. Безопасность на прикладном уровне: PGP и S/MIME.
17. Безопасность на транспортном уровне: SSL и TLS.
18. Безопасность на сетевом уровне: IP SEC.
19. Брандмауэры. Определение типов брандмауэров.
20. Разработка конфигурации межсетевого экрана.
21. Построение набора правил межсетевого экрана.
22. Система обнаружения вторжений (IDS).
23. Узловые IDS. Анализаторы журналов. Датчики признаков.
24. Анализаторы системных вызовов.
25. Анализаторы поведения приложений.
26. Контроллеры целостности файлов.
27. Сетевые IDS. Установка IDS.
28. Определение целей применения IDS. Управление IDS

*Примерные практические задания (задачи) для подготовки к зачету*

**§ 1 Теоретические основы информационной безопасности**

**Задание №1.** Основы защиты ПК

Очистка корзины и **окончательное** удаление файлов.

- Щелкните правой кнопкой мыши на значке **Корзина** на рабочем столе.
- В контекстном меню выберите команду **Свойства.** Отобразится диалоговое окно **Свойства: Корзина.**
- Выберите вкладку **Глобальные**
- Установите флажок **Уничтожать файлы сразу после удаления, не помещая их в корзину**
- Щелкните на кнопке **О К.**

Проверка того, открывал ли кто-нибудь ваш файл во время вашего отсутствия.

- Запустите **Проводник,** выбрав его в меню **Программы** из меню **Пуск**
- Откройте каталог, в котором хранится ваш файл.
- Щелкните на имени файла правой кнопкой мыши, и в отобразившемся контекстном меню выберите команду **Свойства.**

Удаление своих "следов” из меню Документы.

- Выполните команду **Пуск>Настройка>Панель задач и меню "Пуск.** Отобразится диалоговое окно **Свойства: Панель задач.**
- В диалоговом окне **Свойства: Панель задач** выберите **Настройка меню** и щелкните на кнопке **Очистить** в области **Меню "Документы".**

§ 2 Методология защиты информации**Задание № 1.** Простые установки и настройки системы защиты

Удаление и переименование пунктов меню **Пуск.**

- Удалите из меню **Пуск** игру **Косынка.** Очистить **Корзину.**
- Запустите игру **Косынка** (файл Sol.exe)
- Восстановите ярлык **Косынка** в меню **Пуск** на прежнем месте.
- Переименуйте в меню **Пуск** игру **Косынка** на SOL

Скрытие **Панели задач**

- Щелкните на кнопке **Пуск**
- Щелчком мыши выберите **Настройка** > **Панель задач** и откройте диалоговое окно **Свойства: Панель задач.**
- Щелкнете на вкладке **Параметры** панели задач, если это необходимо.
- Щелкните на флажке с надписью **Автоматически убирать с экрана** и на кнопке **ОК.**
- Восстановите **Панель задач**

Зашита от изменения файлов

- Запустите **Проводник.**
- Откройте соответствующую папку и правым щелчком мыши выберите предохраняемый вами файл. Далее выберите пункт **Свойства** в отобразившемся контекстном меню.
- Щелкните на флажке, отмеченном **Только чтение,** и на кнопке **ОК.** Теперь файл защищен от редактирующих его содержимое изменений.

## § 3 Криптографические способы защиты информации

**Задание № 1.** Шифрование и дешифрование данных с помощью программ

- Получить из Интернета и установить бесплатную программу Pretty Good Privacy (PGP) (www.web.mit.edu/network/pgp.html).
- Создать цифровую подпись
- Создать и разместить на сервере свой открытый ключ
- Зашифровать свой файл и отправить его на свой почтовый адрес
- Получить по почте и расшифровать свой файл, используя закрытый ключ.

## § 4. Антивирусная защита

**Задание № 1.** Защита от вирусов

- Установите на компьютере с компакт-диска антивирусную программу Doctor Web (Norton Antivirus, Antiviral Toolkit Pro)
- •Установите параметры программы Doctor Web (Norton Antivirus, Antiviral Toolkit Pro)
- Проверьте дискеты на наличие вирусов
- Вылечите или удалите зараженные файлы

**Задание № 2**. Защита в Интернет

- Проверить безопасность посещаемого вами узла Web. (В обозревателе Internet Explorer выбрать в меню **Сервис** пункт **Свойства обозревателя** и щелкнуть на вкладке **Безопасность).**
- Просмотреть предысторию вашей работы в Интернет (кнопка **Журнал** или **Вид** > **Панели обозревателя** > **Журнал).** Удалить посещенные **вами** адреса URL
- Скрыть поле **Адресная строка** браузера Internet Explorer - через правую кнопку мыши
- Удалите временные файлы Интернета (В обозревателе Internet Explorer выбрать в меню **Сервис** пункт **Свойства обозревателя,** щелкнуть на вкладке **Общие** и на кнопке **Удалить).**
- Устраните файлы cookie (В обозревателе Internet Explorer выбрать в меню **Сервис** пункт **Свойства обозревателя,** щелкнуть на вкладке **Безопасность** и на кнопке **Другой).**
- Восстановите Адресную строку браузера и файлы cookie

## § 5. Сетевая безопасность

**Задание №1.** Применение межсетевого экрана.

1. Запустим на основной машине утилиту поиска уязвимостей PT-Checks:

2. После запуска выберем все три доступных для проверки уязвимости и укажем адрес машины, на которой будем их искать. После проверки можно будет увидеть примерно следующее: То есть две уязвимости из трех на виртуальной машине есть и могут быть использованы для удаленной (сканер ведь тоже обращался по сети) атаки.

3. Включим на виртуальной машине простейший межсетевой экран, который входит в комплект системы. Для этого: вызываем свойства сетевого адаптера, на закладке "Общие" вызываем "Свойства", в свойствах на закладке "Дополнительно" вызываем окно настройки параметров брандмауэра и включаем его:

4. Снова запустим проверку с теми же параметрами: Как видим, уязвимости недоступны.

Выводы: Следует понимать, что мы сделали далеко не все необходимое:

1. Использованный нами сканер - очень узконаправленный. Он обнаруживает только три уязвимости и не использует сложных методов обхода ограничений доступа. Таким образом, мы должны допускать, что есть и другие, неизвестные нам проблемы.

2. Уязвимости после включения никуда не делись. Мы только ограничили к ним доступ и, если брандмауэр сделает исключения для каких-то узлов или сетей - атака оттуда станет возможной. Кроме того, между началом работы машины с сетью и запуском брандмауэра проходит некоторое время - вполне достаточное для поражения.

3. Ошибки и/или злонамеренные действия пользователя вообще не могут быть обнаружены средствами такого типа.

*Примерный билет зачета*

| | | |
|---|---|---|
| Уральский институт ГПС МЧС России | БИЛЕТ № __<br>Кафедра математики и информатики дисциплина «Основы защиты информации», « Информационные системы защиты данны» | УТВЕРЖДАЮ<br><br>Начальник кафедры математики и информатики<br>_____<br>Ф.И.О.<br>«___» _____ 20_ г. |
| 1. Вопросы.<br>1. Защита человека от опасной информации и от не информированности в области информационной безопасности.<br>2. Анализ существующих методик определения требований к защите информации.<br>2. Практическое задание.<br>Перехват передаваемых данных<br>1. Установите на Вашей виртуальной машине анализатор Wireshark. Учтите, что для ее установки и использования необходимо иметь административные права.<br>2. Запустите программу на перехват пакетов в течение 15 секунд.<br>3. Обратите внимание на адреса отправителей и получателей. Если сеть функционирует на базе обычного концентратора, то помимо пакетов, содержащих Ваш адрес, там будут и другие пакеты. Изучите интерфейс программы, чтобы понимать какие данные где отображаются. | | |

**Критерии оценивания зачета**

Зачтено:

- полный и правильный ответ на вопросы (от 90 % до 100 %), успешное решение задачи с необходимыми пояснениями;
- недостаточно полный ответ на вопросы (от 75 % до 89 %); допущены несущественные ошибки при решении задачи;
- в целом ответ на вопросы отражает фрагментарное понимание обучающимся выносимых тем на проверку (от 60 % до 74 %). Допущены ошибки при решении задачи, исправленные после наводящих вопросов.

Не зачтено

- ответы на вопросы отражают незнание обучающимся выносимых тем на проверку (менее 60 %). Обучающийся не владеет навыками решения задач.

## ЛИТЕРАТУРА

Основная литература

1. Кудинов, Ю. И. Основы современной информатики : учебное пособие / Ю. И. Кудинов, Ф. Ф. Пащенко. — 5-е изд., стер. — Санкт-Петербург : Лань, 2022. — 256 с. — ISBN 978-5-8114-0918-1. — Текст : электронный // Лань : электронно-библиотечная система. — URL: https://e.lanbook.com/book/213647

Дополнительная литература

1. Гультяева, Т. А. Основы защиты информации : учебное пособие / Т. А. Гультяева. —Новосибирск : НГТУ, 2018. — 83 с. — ISBN 978-5-7782-3641-7. — Текст : электронный // Лань : ЭБС. — URL: https://e.lanbook.com/book/118234
2. Нестеров, С. А. Основы информационной безопасности : учебное пособие / С. А. Нестеров. — 5-е изд., стер. — Санкт-Петербург : Лань, 2019. — 324 с. — ISBN 978-5-8114-4067-2. —Текст : электронный // Лань : ЭБС. — URL: https://e.lanbook.com/book/114688

## РЕСУРСЫ ИНФОРМАЦИОННО-ТЕЛЕКОММУНИКАЦИОННОЙ СЕТИ «ИНТЕРНЕТ», ПРОФЕССИОНАЛЬНЫЕ БАЗЫ ДАННЫХ И ИНФОРМАЦИОННО-СПРАВОЧНЫЕ СИСТЕМЫ НЕОБХОДИМЫЕ ДЛЯ ОСВОЕНИЯ ДИСЦИПЛИНЫ

1. Информационные системы, реестры, базы и банки данных – Официальный сайт ВНИИПО. – Режим доступа : http://www.vniipo.ru/institut/informatsionnye-sistemy-reestry-bazy-i-banki-danny/
2. Информационно-справочная система «Консультант +» и др. программное обеспечение (при наличии права использования и применения).
3. СДО Прометей - https://dot.uigps.ru/close/default.asp
4. СДО To-Study – sdo.uigps.ru/www/professor.php