МЧС РОССИИ

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 организации самостоятельной работы

20.05.01 Пожарная безопасность
20.03.01 Техносферная безопасность



Екатеринбург
2022

Информационные системы защиты данных. Основы защиты информации [Текст] : Методические рекомендации по организации самостоятельной работы. Специальность 20.05.01 Пожарная безопасность Направление подготовки 20.03.01 Техносферная безопасность / сост. С.А. Худякова, А.В. Шпаньков, Л.В. Якупова – Екатеринбург : Уральский институт ГПС МЧС России, 2022. – 12 с.

Составители:

Худякова С.А., начальник кафедры математики и информатики Уральского института ГПС МЧС России, кандидат педагогических наук, доцент.

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

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

Методические рекомендации по организации самостоятельной работы дисциплины «Информатика» предназначены для обучающихся по специальности 20.05.01 Пожарная безопасность и направление подготовки 20.03.01 Техносферная безопасность и составлены в соответствии с федеральным государственным образовательным стандартом среднего общего образования и рабочей (учебной) программой дисциплины «Информатика».

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

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

СОДЕРЖАНИЕ

ВВЕДЕНИЕ 4
Глава I. Требования к результатам освоения дисциплины 7
Глава II. Структура дисциплины 8
Глава III. Материал и задания для самостоятельной работы по темам дисциплины 8
§ 1 Теоретические основы информационной безопасности 8
§ 2 Методология защиты информации 9
§ 3 Криптографические способы защиты информации 9
§ 4 Антивирусная защита 10
§ 5. Сетевая безопасность 10
ЛИТЕРАТУРА 12

ВВЕДЕНИЕ

Методические рекомендации по организации самостоятельной работы 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 дисциплин «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.

Учебная дисциплины «Информационные системы защиты данных», «Основы защиты данных» включает темы:

Теоретические основы информационной безопасности

Методология защиты информации

Криптографические способы защиты информации

Антивирусная защита

Сетевая безопасность

Изучение дисциплин «Информационные системы защиты данных», «Основы защиты данных» в 6 семестре завершается зачетом в рамках промежуточной аттестации.

Самостоятельная работа обучающихся является одним из видов учебных занятий. Она определяется как индивидуальная или групповая учебная деятельность, осуществляемая без непосредственного руководства педагога, но по его заданиям и под его контролем.

Самостоятельная работа обучающихся является одной из основных форм

внеаудиторной работы. По дисциплинам «Информационные системы защиты данных», «Основы защиты данных» применяются следующие виды и формы самостоятельной работы:

– отработка изучаемого материала по печатным и электронным источникам, конспектам лекций;

– изучение лекционного материала по конспекту с использованием рекомендованной литературы;

– решение практических задач.

Самостоятельная работа проводится с целью:

– систематизации и закрепления полученных теоретических знаний и практических умений;

– углубления и расширения теоретических знаний;

– формирования умений использовать справочную и дополнительную литературу;

– формирования самостоятельности мышления, способностей к саморазвитию, самосовершенствованию и самореализации.

Самостоятельная внеаудиторная работа выполняется обучающимися по заданию ведущего педагога, но без его непосредственного участия. Руководством для выполнения заданий служат учебные пособия, интернет-ресурсы.

Виды самостоятельных работ

В учебном процессе выделяют два вида самостоятельной работы:

- аудиторная;
- внеаудиторная.

Аудиторная самостоятельная работа по дисциплине выполняется на лекционных и практических занятиях под непосредственным руководством педагога и по его заданию.

Внеаудиторная самостоятельная работа выполняется обучающимися по заданию педагога, но без его непосредственного участия.

Содержание аудиторной и внеаудиторной самостоятельной работы определяется рабочей (учебной) программы учебной дисциплины.

Виды заданий для аудиторной самостоятельной работы

1. Выполнение упражнений по образцу.
2. Выполнение тестовых заданий.
3. Выполнение контрольных работ.

Виды заданий для внеаудиторной самостоятельной работы

1. Чтение текста учебной литературы, работа со справочной литературой, использование интернет-ресурсов и другое.
2. Работа с конспектом лекции, обработка текста, повторная работа над учебным материалом, ответы на вопросы, вынесенные на самостоятельное изучение, решение задач по образцу и другое.

Самостоятельная работа может осуществляться индивидуально или коллективом обучающихся – в зависимости от цели, объема, конкретной тематики самостоятельной работы, уровня сложности, уровня умений обучающихся.

Контроль результатов внеаудиторной самостоятельной работы обучающихся может осуществляться в пределах времени, отведенного на аудиторные учебные занятия. Контроль может проходить в письменной, устной или смешанной форме.

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 деятельности, демонстрировать навыки правовой культуры	**ПК-19**. Способен планировать, организовывать и осуществлять комплекс контрольных (надзорных) мероприятий за соблюдением обязательных требований пожарной безопасности и другие контрольно-надзорные функции, квалификацию правонарушений в области пожарной безопасности с учетом степени риска причинения вреда охраняемым законом ценностям.	**Знать:** основы нормативного правового регулирования информационных систем защиты данных. **Уметь:** применять законодательство, регулирующее отношения в области информационных систем защиты данных. **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. Материал и задания для самостоятельной работы по темам дисциплины

В данном разделе приведены вопросы и типовые задания (задачи), которые помогут более качественно подготовиться к различным контрольным мероприятиям.

§ 1 Теоретические основы информационной безопасности

I. Составить конспект по вопросам:
1. Программные и программно-аппаратные методы и средства обеспечения информационной безопасности.
2. Модель интеграции информационной безопасности в основную деятельность организации.
3. Понятие Политики безопасности.

II. Решить задачи

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

I. Составить конспект по вопросам:

1. Анализ существующих методик определения требований к защите информации.
2. Система сертификации РФ в области защиты информации.
3. Основные правила и документы системы сертификации РФ в области защиты информации

II. Решить задачи

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

I. Составить конспект по вопросам:

1. Шифрование с помощью аналитических преобразований. Комбинированные методы шифрования.
2. Стандарты шифрования.
3. Стандарт шифрования данных Data Encryption Standard.

4. Режимы работы алгоритма DES.
5. Алгоритм шифрования данных IDEA.
6. Общая схема алгоритма IDEA

II. Решить задачи

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

I. Составить конспект по вопросам:

1. Общие понятия антивирусной защиты.
2. Уязвимости.
3. Классификация вредоносных программ.
4. Признаки присутствия на компьютере вредоносных программ.
5. Методы защиты от вредоносных программ.

II. Решить задачи

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

§ 5. Сетевая безопасность

I. Составить конспект по вопросам:

1. Узловые IDS. Анализаторы журналов. Датчики признаков.
2. Анализаторы системных вызовов.
3. Анализаторы поведения приложений.
4. Контроллеры целостности файлов.
5. Сетевые IDS. Установка IDS.
6. Определение целей применения IDS. Управление IDS

II. Решить задачи

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.

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