



УТВЕРЖДЕНО:

Ученым советом Института сервисных технологий ФГБОУ ВО «РГУТИС»
Протокол № 10 от «24» февраля 2021г.
с изм. Протокол № 11 от «16» апреля 2021г.
с изм. Протокол № 14 от «30» июня 2021г.

**МЕТОДИЧЕСКИЕ УКАЗАНИЯ ПО ОСВОЕНИЮ
ДИСЦИПЛИНЫ**

ОП.В.02 ИНФОРМАЦИОННАЯ БЕЗОПАСНОСТЬ

основной профессиональной образовательной программы среднего профессионального образования – программы подготовки специалистов среднего звена по специальности: *09.02.07 Информационные системы и программирование*
Квалификация: *специалист по информационным системам*

год начала подготовки: 2021

Разработчики:

должность	подпись	ученая степень и звание, ФИО
<i>преподаватель</i>		<i>Дуденков П.А.</i>

Методические указания согласованы и одобрены руководителем ШССЗ:

должность	подпись	ученая степень и звание, ФИО
<i>преподаватель</i>		<i>к.м.н. Алабина С.А.</i>



СОДЕРЖАНИЕ

1. Общие положения.....	3
2. Тематика и содержание лекций.....	5
3. Тематика и содержание практических занятий	6
4. Тематика и содержание самостоятельной работы.....	7
5. Информационное обеспечение обучения.....	9



1. Общие положения

Методические указания предназначены для обучающихся по ООП СПО по специальности 09.02.07 Информационные системы и программирование, изучающих учебную дисциплину «Информационная безопасность», и могут использоваться как на учебных занятиях, которые проводятся под руководством преподавателя, так и для самостоятельного выполнения практических работ, предусмотренных рабочей программой во внеаудиторное время.

Цели и задачи освоения дисциплины: «Информационная безопасность»

Содержание учебной дисциплины ориентировано на подготовку студентов к освоению специальности 09.02.07 «Информационные системы и программирование» и овладению общими компетенциями (ОК):

ОК 01.	Выбирать способы решения задач профессиональной деятельности, применительно к различным контекстам.
ОК 02.	Осуществлять поиск, анализ и интерпретацию информации, необходимой для выполнения задач профессиональной деятельности.
ОК 04.	Работать в коллективе и команде, эффективно взаимодействовать с коллегами, руководством, клиентами.
ОК 05.	Осуществлять устную и письменную коммуникацию на государственном языке с учетом особенностей социального и культурного контекста.
ОК 09.	Использовать информационные технологии в профессиональной деятельности.
ОК 10.	Пользоваться профессиональной документацией на государственном и иностранном языке.

Виды занятий.

В рамках освоения дисциплины реализуются следующие виды занятий:

Лекционные занятия.

Практические занятия.

В результате освоения учебной дисциплины обучающийся должен уметь:

- применять методы и системы защиты информации;
- обеспечивать защиту и сохранность данных в сети,



- своевременно реагировать на вирусные угрозы и кибератаки;
- принимать участие в эксплуатации подсистем управления информационной безопасностью различных объектов информатизации;
- администрировать подсистемы информационной безопасности различных объектов информатизации;

В результате освоения учебной дисциплины обучающийся должен знать:

- сущность, цели и принципы информационной безопасности, законодательные основы ее реализации;
- информационно-правовые аспекты безопасности информационных ресурсов, принципы и способы охраны интеллектуальной собственности;
- направления и методы обеспечения безопасности информационных ресурсов, ведения аналитической работы по выявлению угроз несанкционированного доступа к информации, ее утраты;
- методику защиты информации в деятельности организации;
- функциональные возможности и предпосылки эффективного использования различных типов технологических систем и способов обработки и хранения традиционных и электронных конфиденциальных документов.

Формы контроля

В процессе изучения дисциплины предусмотрены следующие формы контроля по овладению общекультурными и профессиональными компетенциями: текущий контроль в форме практических работ, устных опросов, самостоятельной работы обучающихся промежуточный контроль в форме экзамена.

Текущий контроль осуществляется в течение семестра в виде оценки результатов практических занятий, оценки выполнения самостоятельных работ, оценки устного опроса.

Промежуточная аттестация экзамен в 7 семестре

Контроль самостоятельной работы студентов осуществляется в течение всего семестра. Преподаватель самостоятельно определяет формы контроля самостоятельной работы студентов в зависимости от содержания разделов и тем, выносимых на самостоятельное изучение. Такими формами могут являться: тестирование, видеопрезентации, проектные технологии, контрольные работы и др.

2. Тематика и содержание лекций

Лекция – один из методов обучения, одна из основных системообразующих форм организации учебного процесса.

Лекционное занятие представляет собой систематическое, последовательное, монологическое изложение преподавателем-лектором



учебного материала, как правило, теоретического характера. Такое занятие представляет собой элемент технологии представления учебного материала путем логически стройного, систематически последовательного и ясного изложения.

Цель лекции – организация целенаправленной познавательной деятельности студентов по овладению программным материалом учебной дисциплины.

Тематика и содержание

Тема 1. Концепции и аспекты обеспечения информационной безопасности

1. Понятия экономической и информационной безопасности.
2. Ключевые вопросы информационной безопасности

Тема 2. Виды угроз информационной безопасности

1. Виды угроз информационной безопасности
2. Основные виды защищаемой информации

Тема 3. Построения системы информационной безопасности

1. Основные аспекты построения системы информационной безопасности
2. Анализ и управление рисками при реализации информационной безопасности

Тема 4. Защита информации в информационных системах и компьютерных сетях

1. Защита информации в информационных системах и компьютерных сетях.
2. Методология анализа защищенности информационной системы.

Тема 5. Обеспечение безопасности ИС

1. Требования к архитектуре ИС для обеспечения безопасности ее функционирования.
2. Технологии криптографической защиты информации. Современные средства биометрической идентификации.

Тема 6. Обеспечение интегральной безопасности ИС

1. Обеспечение интегральной безопасности информационных систем и сетей
2. Технологии криптографической защиты информации.

3. Тематика и содержание практических занятий



Тема 2. Виды угроз информационной безопасности

Практическое занятие 1.

«Основы законодательства в области обеспечения информационной безопасности».

Практическое занятие 2.

«Разработка метода и модели системы защиты информации».

Практическое занятие 3.

«Алгоритм проведения анализа и оценки угроз».

Тема 3. Построения системы информационной безопасности

Практическое занятие 1.

«Адаптивная модель СЗИ на базе нейронных сетей».

Практическое занятие 2.

«Схема работы генетического алгоритма».

Тема 4. Защита информации в информационных системах и компьютерных сетях

Практическое занятие 1.

«Адаптивная модель СЗИ на базе нейронных сетей».

Практическое занятие 2.

«Схема работы генетического алгоритма».

Тема 5. Обеспечение безопасности ИС

Практическое занятие 1.

«Защита информации в распределенной ИС».

Практическое занятие 2.

«Шифрование и дешифрование данных. Таблица Вижинера».

Тема 6. Обеспечение интегральной безопасности ИС

Практическое занятие 1.

«Распределенная информационная система».

Практическое занятие 2.

«Технологии токенов».

Практическое занятие 3.

«Компоновка VPN на основе международных стандартов и протоколов».

4. Тематика и содержание самостоятельной работы

Самостоятельная работа является неотъемлемой частью образовательного процесса, связанного с формированием компетенций обучающихся

Целью самостоятельной (внеаудиторной) работы студентов является обучение навыкам работы с научно-теоретической, периодической, научно-технической литературой и технической документацией, необходимыми для углубленного изучения дисциплины, а также развитие у них устойчивых способностей к самостоятельному изучению и изложению полученной



информации.

Формы (виды) самостоятельной работы

Самостоятельная работа выполняется в форме подготовки доклада по теме, выполнения тестовых заданий.

Тематика и содержание

Примерные темы докладов

- 1) Основные термины и определения безопасности и защиты информации
- 2) Сущность и понятие информационной безопасности и защиты информации
- 3) Цели и концептуальные основы информационной безопасности и защиты информации
- 4) Принцип историчности в системах безопасности и защиты информации
- 5) Конфиденциальная информация. Классификация по видам и степеням конфиденциальности
- 6) Носители защищаемой информации
- 7) Потенциальные угрозы защищаемой информации. Виды и методы дестабилизирующего воздействия на защищаемую информацию.
- 8) Элементарная и многозвенная модель защиты информации
- 9) Модель многоуровневой защиты
- 10) Комплексная вероятностная модель защиты информации
- 11) Расчет надежности защиты информации
- 12) Законодательные средства защиты информации
- 13) Организационно-законодательные средства защиты информации
- 14) Физические средства защиты информации
- 15) Аппаратные средства защиты информации
- 16) Программные и криптографические средства защиты информации
- 17) Порядок определения комплекса средств защиты информации для объекта информатизации
- 18) Основные положения криптографии. Теоретическая и практическая стойкость шифров. Допущения Шеннона
- 19) Методы криптографического преобразования данных.
Перестановка.
- 20) Методы криптографического преобразования данных.
Гаммирование.
- 21) Методы криптографического преобразования данных.
Аналитические преобразования.



- 22) Основные положения построения симметричных и несимметричных криптосистем
- 23) Однонаправленные функции
- 24) Практическое применение шифров. Таблица Вижинера.
- 25) Практическое применение шифров. Таблица Метод RSA.
- 26) Виды и сущность криптоанализа. Правило Киркхоффа
- 27) Понятие и основные положения цифровой стеганографии
- 28) Принципы организации разноуровневого доступа в автоматизированных информационных системах.
- 29) Понятие несанкционированного доступа и защита от него.
- 30) Управление доступом в информационных системах. Основные понятия: клиент, право и объект доступа, группы, роли, политика безопасности.
- 31) Дискреционная модель доступа. Преимущества и недостатки.
- 32) Мандатная модель доступа. Преимущества и недостатки.
- 33) Сущность и проявление РПС (компьютерных вирусов).
- 34) Классификация компьютерных вирусов.
- 35) Основные виды вирусов и схемы их функционирования.
- 36) Программы обнаружения и защиты от вирусов, особенности их работы.

5. Информационное обеспечение обучения.

Перечень рекомендуемых учебных изданий, Интернет-ресурсов, дополнительной литературы


Основные источники:

Партыка, Т. Л. Информационная безопасность : учебное пособие / Т.Л. Партыка, И.И. Попов. — 5-е изд., перераб. и доп. — Москва : ФОРУМ : ИНФРА-М, 2021. — 432 с. — (Среднее профессиональное образование). - URL: <https://znanium.com/catalog/product/1189328>

2. Васильков, А. В. Безопасность и управление доступом в информационных системах : учебное пособие / А.В. Васильков, И.А. Васильков. — Москва : ФОРУМ : ИНФРА-М, 2020. — 368 с. — (Среднее профессиональное образование). - URL: <https://znanium.com/catalog/product/1082470>

Дополнительные источники:

1. Шаньгин, В. Ф. Информационная безопасность компьютерных систем и сетей : учебное пособие / В.Ф. Шаньгин. — Москва : ФОРУМ : ИНФРА-М, 2021. — 416 с. — (Среднее профессиональное образование). - URL: <https://znanium.com/catalog/product/1189327>

	ФЕДЕРАЛЬНОЕ ГОСУДАРСТВЕННОЕ БЮДЖЕТНОЕ ОБРАЗОВАТЕЛЬНОЕ УЧРЕЖДЕНИЕ ВЫСШЕГО ОБРАЗОВАНИЯ «РОССИЙСКИЙ ГОСУДАРСТВЕННЫЙ УНИВЕРСИТЕТ ТУРИЗМА И СЕРВИСА»	СК РГУТИС ...
		Лист 9

2. Информационная безопасность : учебник / Мельников В.П., под ред., Куприянов А.И. — Москва : КноРус, 2021. — 267 с.— URL: <https://book.ru/book/939292>

Интернет – ресурсы:

1. Научно-технический и научно-производственный журнал «Информационные технологии» <http://novtex.ru/IT/index.htm>
2. Журнал «Информационное общество» <http://www.infosoc.iis.ru/>
3. Журнал «Бизнес-информатика» <https://bijournal.hse.ru/>
4. Журнал «Информационные системы и технологии» <http://oreluniver.ru/science/journal/isit>
5. Журнал «Электронные информационные системы». Режим доступа: <https://elins-journal.ru/>