МИНОБРНАУКИ РОССИИ

Федеральное государственное автономное образовательное учреждение

высшего образования

«Российский государственный гуманитарный университет»
(ФГАОУ ВО «РГГУ»)

ИНСТИТУТ ИНФОРМАЦИОННЫХ НАУК И ТЕХНОЛОГИЙ БЕЗОПАСНОСТИ
Факультет информационных систем и безопасности

Кафедра информационной безопасности

ЗАЩИТА ИНФОРМАЦИИ ОТ НЕСАНКЦИОНИРОВАННОГО ДОСТУПА

РАБОЧАЯ ПРОГРАММА ДИСЦИПЛИНЫ

46.03.02 Документоведение и архивоведение
Код и наименование направления подготовки/специальности

Интеллектуальные системы в управлении документами
Наименование направленности (профиля)/ специализации

Уровень высшего образования: *бакалавриат*

Форма обучения: *очная*

РПД адаптирована для лиц
с ограниченными возможностями
здоровья и инвалидов

Москва 2025

Защита информации от несанкционированного доступа
Рабочая программа дисциплины
Составитель(и):
Канд. ист. наук, доцент,
доцент кафедры ИБ Г.А. Шевцова

Ответственный редактор
Д.и.н., профессор, зав кафедрой АС ДОУ М.В. Ларин

УТВЕРЖДЕНО
Протокол заседания кафедры
информационной безопасности
№ 3 от 30.10.2024

ОГЛАВЛЕНИЕ

1 Пояснительная записка

1.1 Цель и задачи дисциплины

Цель дисциплины – получение знаний по существующим угрозам информационной безопасности, применению современных методов и способов защиты информации от несанкционированного доступа (НСД); формирование навыков, необходимых для защиты информации от НСД в современных информационных системах.

Задачи дисциплины:
– овладение методами решения профессиональных задач по защите информации от НСД;
– формирование навыков работы с современными средствами защиты информации от НСД;
– обоснования выбора способов защиты информации от НСД в информационных системах;
– изучение основ анализа угроз безопасности информации;
– развитие комплексного мышления и умения анализировать ситуацию.

1.2 Перечень планируемых результатов обучения по дисциплине, соотнесенных с индикаторами достижения компетенций

Компетенции	**Индикаторы компетенций**	**Результаты обучения по дисциплине**
ОПК 5. Способен самостоятельно работать с различными источниками информации и применять основы информационно-аналитической деятельности при решении профессиональных задач	ОПК-5.1 Владеет основными принципами работы с источниками информации, принципами сбора, анализа и обработки информации	Знать: особенности и назначение используемого программного обеспечения Уметь: применять основы информационно-аналитической деятельности при решении профессиональных задач Владеть: навыками использования информационных ресурсов к программным системам и стандартам в области программирования и информационных систем
ОПК-7. Способен к профессиональному росту и самосовершенствовани ю в области гуманитарных, социальных и лингвистических наук, а также в сфере техники и технологии информатики	ОПК-7.1. Знает методы доступа к информационным ресурсам	Знать: ресурсы и ограничения имеющегося программного обеспечения Уметь: применять основы информационно-аналитической деятельности при решении профессиональных задач Владеть: навыками использования информационных ресурсов к программным системам и стандартам в области программирования и информационных систем

ПК-2. Способен организовать работу с документацией в организациях различных организационно-правовых форм	ПК-2.2. Знает законодательные и нормативно-правовые акты Российской Федерации в сфере управления документами, в области информации, информационных технологий и защиты информации, персональных данных и цифровой трансформации	Знать: законодательные и нормативно-правовые акты Российской Федерации в сфере управления документами, в области информации, информационных технологий и защиты информации, персональных данных и цифровой трансформации Уметь: разрабатывать локальные нормативные акты в сфере управления документами, в области информации, информационных технологий и защиты информации, персональных данных и цифровой трансформации Владеть: навыками подготовки проектов документов с использованием законодательных и нормативно-правовых актов Российской Федерации в сфере управления документами, в области информации, информационных технологий и защиты информации, персональных данных и цифровой трансформации
ПК-4. Способен осуществлять проектирование и внедрение систем электронного документооборота в организации	ПК-4.1. Обеспечивает доступ пользователей и ведение информационно-справочной работы в информационной системе	Знать: современные информационные системы, системы электронного документооборота, правовое регулирование сферы управления информацией и документацией Уметь: применять знание информационно-справочной базы в сфере управления информацией и документацией в практической деятельности Владеть: навыками выбора необходимых технологический решений в процессе информационно-справочной работы в информационной системе
	ПК-4.3. Способен определять требования к системам электронного документооборота по сохранности и защите цифрового контента	Знать: правила и методологические подходы к системам электронного документооборота по сохранности и защите цифрового контента Уметь: пользоваться в системах электронного документооборота технологиями защиты цифрового контента Владеть: навыками определения требований к системам электронного документооборота по сохранности и защите цифрового контента

1.3 Место дисциплины в структуре основной образовательной программы

Дисциплина *«Защита информации от несанкционированного доступа»* относится к базовой части блока дисциплин учебного плана.

Для освоения дисциплины необходимы знания, умения и владения, сформированные в ходе изучения следующих дисциплин и прохождения практик: «Разработка информационных систем», «Информационные технологии в архивном деле», «Технологии искусственного интеллекта в управлении документами».

В результате освоения дисциплины формируются знания, умения и владения, необходимые для изучения следующих дисциплин и прохождения практик: «Форматы электронных документов в системах электронного документооборота», «Государственные информационные системы», преддипломная практика, государственная итоговая аттестация.

2 Структура дисциплины

Общая трудоемкость дисциплины составляет 3 з.е., 108 ч.

Структура дисциплины для очной формы обучения

Объем дисциплины в форме контактной работы обучающихся с педагогическими работниками и (или) лицами, привлекаемыми к реализации образовательной программы на иных условиях, при проведении учебных занятий:

Семестр	Тип учебных занятий	Количество часов
2	Лекции	**16**
2	Семинары/лабораторные работы	**24**
	Всего:	**40**

Объем дисциплины в форме самостоятельной работы обучающихся составляет 68 академических часов.

3 Содержание дисциплины

Тема 1. Введение в защиту информации от несанкционированного доступа

Основные термины и определения ЗИ от НСД. Классификация требований к системам защиты от НСД. Ответственность за НСД. Документы Гостехкомиссии (ФСТЭК) России по защите от НСД. Система государственных нормативных актов, стандартов, руководящих документов и требований по защите информации от НСД. Особенности современных автоматизированных систем. Виды угроз современным автоматизированным системам (АС). Классы защищённости СВТ и АС. Показатели защищённости межсетевых экранов и их увязка с классами защищённости АС.

Тема 2. Требования к защите информации от несанкционированного доступа Авторизация. Методы идентификации и аутентификации пользователя

Формализованные требования к защите информации от НСД. Классы защищённости СВТ. Классификация автоматизированных систем по защищённости от НСД. Состав первой группы защиты автоматизированных систем. Подсистемы механизма защиты информации от НСД. Требования к защите информации автоматизированных систем групп 1Г и 1В.

Понятие идентификации и аутентификации. Процедура авторизации. Формализованные и дополнительные требования к идентификации и аутентификации. Авторизация в контексте количества и вида зарегистрированных пользователей. Рекомендации по построению авторизации, исходя из вида и количества зарегистрированных пользователей. Классификация задач, решаемых механизмами идентификации и аутентификации. Критерии классификации. Механизмы парольной защиты. Функциональное назначение и реализация механизмов парольной защиты. Угрозы преодоления парольной защиты. Явные и скрытые угрозы. Основные механизмы ввода пароля. Биометрический и комбинированный способ ввода пароля. Способы усиления парольной защиты. Добавочные механизмы усиления парольной защиты и требования к ним. Двухуровневая авторизация на уровне ОС и BIOS. Сетевая авторизация. Протоколы аутентификации.

Тема 3. Управление доступом к ресурсам

Основные способы разделения доступа субъектов к совместно используемым объектам. Абстрактные модели доступа. Модели Биба, Гогена-Мезигера, Кларка-Вильсона, Сазерлендская модель. Дискреционная (матричная) модель. Многоуровневые (мандатные) модели. Понятия «владелец» и «собственник» информации.

Базовые модели доступа. Дискреционное разграничение доступа. Матрица доступа и домен безопасности. Список прав доступа ACL. Мандатное разграничение доступа. Ролевая модель разграничения доступа. Управления доступом на основе атрибутов. Выбор модели разграничения доступа.

Корректность и полнота реализации разграничительной политики доступа. Классификация субъектов и объектов доступа. Требования к механизмам управления доступом.

Централизованное и децентрализованное управление доступом. Протоколы аутентификации (AAA). RADIUS, TACACS.

Тема 4. Разработка политики безопасности информационной системы

Общие положения разработки политики безопасности. Нормативные документы по разработке политики безопасности. Важные аспекты при разработке политик безопасности. Средства защиты информации для государственных и коммерческих структур. Процесс разработки политики безопасности. Примерный состав группы по разработке политик безопасности. Требования к политикам безопасности. Типовые политики безопасности.

Реализация политик безопасности. Общие правила безопасности. Архитектура корпоративной системы защиты информации. Настройки основных компонент системы защиты компании.

Тема 5. Методика анализа защищённости информационных систем (ИС). Методы и средства выявления угроз её информационной безопасности

Типовая методика анализа защищённости ИС. Методы тестирование систем информационной безопасности. Методы количественной оценки систем информационной безопасности. Методы и средства анализа защищённости автоматизированной системы.

Анализ защищённости внешнего периметра корпоративной сети. Анализ защищённости внутренней инфраструктуры сети. Инструментальные средства анализа защищённости. Методы предотвращения сетевых атак на периметр сети.

Тема 6. Применение средств аппаратной защиты

Необходимость и принципы использования аппаратных средств защиты. Угрозы перевода системы защиты в пассивное состояние, их реализация. Методы противодействия угрозам перевода системы защиты в пассивное состояние. Реализация программно-аппаратного контроля (мониторинга) активности системы защиты. Метод контроля целостности и активности программных компонент системы защиты программно-аппаратными средствами. Механизм удалённого мониторинга активности системы защиты, как альтернатива применению аппаратной компоненты защиты. Метод контроля вскрытия аппаратуры, общий подход. Реализация системы контроля вскрытия аппаратуры. Принципы комплексирования средств защиты информации.

4 Образовательные технологии

№ п/п	**Наименование раздела**	**Виды учебных занятий**	**Образовательные технологии**
1	**2**	**3**	**4**
1.	Введение в защиту информации от несанкционированного доступа	Лекция Самостоятельная работа	Лекция с использованием видеоматериалов Работа с литературой
2	Требования к защите информации от несанкционированного доступа. Авторизация. Методы идентификации и аутентификации пользователя	Лекция Семинарские занятия Самостоятельная работа	Лекция с использованием видеоматериалов Прием заданий Работа с литературой
3	Управление доступом к ресурсам	Лекция Семинарские занятия Самостоятельная работа	Лекция с использованием видеоматериалов Прием заданий Работа с литературой
4	Разработка политики безопасности информационной системы	Лекция Семинарские занятия Самостоятельная работа	Лекция с использованием видеоматериалов Прием заданий Работа с литературой
5	Методика анализа защищённости ИС. Методы и средства выявления угроз её информационной безопасности	Лекция Семинарские занятия Самостоятельная работа	Лекция с использованием видеоматериалов Прием заданий Работа с литературой
6	Применение средств аппаратной защиты	Лекция	Лекция с использованием

		Семинарские занятия Самостоятельная работа	видеоматериалов Прием заданий Работа с литературой
7	Комплексный подход при разработке политики безопасности организации	Семинарские занятия Самостоятельная работа	Прием заданий Работа с литературой
8	Анализ система мероприятий, направленных на максимальное предотвращение утечки информации	Семинарские занятия Самостоятельная работа	Прием заданий Работа с литературой
9	Подходы к оценке эффективности систем информационной безопасности	Семинарские занятия Самостоятельная работа	Прием заданий Работа с литературой

В период временного приостановления посещения обучающимися помещений и территории РГГУ для организации учебного процесса с применением электронного обучения и дистанционных образовательных технологий могут быть использованы следующие образовательные технологии:
– видео-лекции;
– онлайн-лекции в режиме реального времени;
– электронные учебники, учебные пособия, научные издания в электронном виде и доступ к иным электронным образовательным ресурсам;
– системы для электронного тестирования;
– консультации с использованием телекоммуникационных средств.

5 Оценка планируемых результатов обучения

5.1 Система оценивания

Форма контроля	**Макс. количество баллов**	
	За одну работу	**Всего**
Текущий контроль: *- опрос (темы 1-6)* *- Семинарские занятия*	 *4 балла* *4 балла*	 *24 баллов* *36 баллов*
Промежуточная аттестация *Устный опрос по билетам*		*40 баллов*
Итого за дисциплину *зачёт*		*100 баллов*

Полученный совокупный результат конвертируется в традиционную шкалу оценок и в шкалу оценок Европейской системы переноса и накопления кредитов (European Credit Transfer System; далее – ECTS) в соответствии с таблицей:

100-балльная шкала	Традиционная шкала		Шкала ECTS
95 – 100	отлично	зачтено	A
83 – 94			B
68 – 82	хорошо		C
56 – 67	удовлетворительно		D
50 – 55			E
20 – 49	неудовлетворительно	не зачтено	FX
0 – 19			F

5.2 Критерии выставления оценки по дисциплине

Баллы/ Шкала ECTS	Оценка по дисциплине	Критерии оценки результатов обучения по дисциплине
100-83/ A,B	«отлично»	Выставляется обучающемуся, если он глубоко и прочно усвоил теоретический и практический материал, может продемонстрировать это на занятиях и в ходе промежуточной аттестации. Обучающийся исчерпывающе и логически стройно излагает учебный материал, умеет увязывать теорию с практикой, справляется с решением задач профессиональной направленности высокого уровня сложности, правильно обосновывает принятые решения. Свободно ориентируется в учебной и профессиональной литературе. Оценка по дисциплине выставляются обучающемуся с учётом результатов текущей и промежуточной аттестации. Компетенции, закреплённые за дисциплиной, сформированы на уровне – «высокий».
82-68/ C	«хорошо»	Выставляется обучающемуся, если он знает теоретический и практический материал, грамотно и по существу излагает его на занятиях и в ходе промежуточной аттестации, не допуская существенных неточностей. Обучающийся правильно применяет теоретические положения при решении практических задач профессиональной направленности разного уровня сложности, владеет необходимыми для этого навыками и приёмами. Достаточно хорошо ориентируется в учебной и профессиональной литературе. Оценка по дисциплине выставляются обучающемуся с учётом результатов текущей и промежуточной аттестации. Компетенции, закреплённые за дисциплиной, сформированы на уровне – «хороший».
67-50/ D,E	«удовлетвори-тельно»	Выставляется обучающемуся, если он знает на базовом уровне теоретический и практический материал, допускает отдельные ошибки при его изложении на занятиях и в ходе промежуточной аттестации. Обучающийся испытывает определённые затруднения в применении теоретических положений при решении практических задач профессиональной направленности стандартного уровня сложности, владеет необходимыми для этого базовыми навыками и приёмами. Демонстрирует достаточный уровень знания учебной литературы по дисциплине.

Баллы/ Шкала ECTS	Оценка по дисциплине	Критерии оценки результатов обучения по дисциплине
		Оценка по дисциплине выставляются обучающемуся с учётом результатов текущей и промежуточной аттестации. Компетенции, закреплённые за дисциплиной, сформированы на уровне – «достаточный».
49-0/ F,FX	«неудовлетворительно»	Выставляется обучающемуся, если он не знает на базовом уровне теоретический и практический материал, допускает грубые ошибки при его изложении на занятиях и в ходе промежуточной аттестации. Обучающийся испытывает серьёзные затруднения в применении теоретических положений при решении практических задач профессиональной направленности стандартного уровня сложности, не владеет необходимыми для этого навыками и приёмами. Демонстрирует фрагментарные знания учебной литературы по дисциплине. Оценка по дисциплине выставляются обучающемуся с учётом результатов текущей и промежуточной аттестации. Компетенции на уровне «достаточный», закреплённые за дисциплиной, не сформированы.

5.3 Оценочные средства (материалы) для текущего контроля успеваемости, промежуточной аттестации обучающихся по дисциплине

При изучении дисциплины «Защита информации от несанкционированного доступа» используется рейтинговая система оценки знаний студентов.

По дисциплине предусматривается текущий и промежуточный контроль. Текущий контроль знаний организуется с использованием набора тестовых заданий. Помимо этого выполнение студентами заданий на семинарских занятиях также контролируется преподавателем.

В качестве форм текущего *контроля* используются также следующие формы:

- собеседование;
- проверка рефератов и письменных докладов;
- проведение опросов – устных и письменных;
- тестирование;
- коллоквиумы;
- проверка конспектов занятий, статей и др.

Формой промежуточной аттестации является зачет.

Прием итогового зачета проводится по билетам лектором потока в форме беседы, предусматривает наличие ответов на теоретические вопросы билета и призван выявить уровень знаний студента по всем темам дисциплины.

Студенты допускаются к сдаче зачета только после выполнения всех видов самостоятельной и аудиторной работы, предусмотренных данной программой.

Перечень вопросов к зачету

1. Назовите и раскройте содержательный смысл документов ФСТЭК (Гостехкомиссии) России по защите от НСД. Система государственных нормативных актов по ЗИ от НСД.
2. Какие виды угроз присутствуют современным АС?
3. Какие классы защищённости СВТ и АС и показатели защищённости межсетевых экранов и их увязка с классами защищённости АС вы знаете?
4. Подсистемы механизма ЗИ от НСД. Какие требования к защите информации АС групп 1Г и 1В?
5. Понятие идентификации и аутентификации. Какова процедура авторизации?
6. Формализованные и дополнительные требования к идентификации и аутентификации. Авторизация в контексте количества и вида зарегистрированных пользователей. Рекомендации по построению авторизации, исходя из вида и количества зарегистрированных пользователей.
7. Раскройте механизмы парольной защиты. Функциональное назначение и реализация механизмов парольной защиты.
8. Какие существуют в настоящее время угрозы преодоления парольной защиты?
9. Какие основные механизмы ввода пароля вы знаете?
10. Двухуровневая авторизация на уровне ОС и BIOS. Сетевая авторизация.
11. Протоколы аутентификации.
12. Абстрактные модели доступа. Понятия «владелец» и «собственник» информации.
13. Дискреционное разграничение доступа.
14. Мандатное разграничение доступа.
15. Ролевая модель разграничения доступа.
16. Управления доступом на основе атрибутов. Выбор модели разграничения доступа.
17. Корректность и полнота реализации разграничительной политики доступа. Классификация субъектов и объектов доступа. Требования к механизмам управления доступом.
18. Централизованное и децентрализованное управление доступом.
19. Общие положения разработки политики безопасности. Нормативные документы по разработке политики безопасности.
20. Процесс разработки политики безопасности. Требования к политикам безопасности.
21. Реализация политик безопасности. Архитектура корпоративной системы защиты информации. Настройки основных компонент системы защиты компании.
22. Типовая методика анализа защищённости ИС
23. Методы количественной оценки систем информационной безопасности.
24. Анализ защищённости внешнего периметра и внутренней инфраструктуры корпоративной сети.
25. Инструментальные средства анализа защищённости. Методы предотвращения сетевых атак на периметр сети.
26. Угрозы перевода системы защиты в пассивное состояние, их реализация. Методы противодействия угрозам перевода системы защиты в пассивное состояние.
27. Реализация программно-аппаратного контроля (мониторинга) активности системы защиты.
28. Метод контроля целостности и активности программных компонент системы защиты программно-аппаратными средствами.
29. Механизм удалённого мониторинга активности системы защиты, как альтернатива применению аппаратной компоненты защиты.
30. Метод контроля вскрытия аппаратуры, общий подход. Реализация системы контроля вскрытия аппаратуры.
31. Принципы комплексирования средств защиты информации

Тестовые задания

1. Для защиты от несанкционированного доступа к программам и данным, хранящимся на компьютере, используются

1) пароли
2) анкеты
3) коды
4) ярлыки

2. От несанкционированного доступа может быть защищён:

Выберите несколько вариантов ответа:
1) каждый диск
2) папка
3) файл
4) ярлык

3. К биометрическим системам защиты информации относятся системы идентификации по:

Выберите несколько вариантов ответа:
1) отпечаткам пальцев
2) характеристикам речи
3) радужной оболочке глаза
4) изображению лица
5) геометрии ладони руки
6) росту
7) весу
8) цвету глаз
9) цвету волос

4. Какие существуют массивы дисков RAID?

Выберите несколько вариантов ответа:
1) RAID 0
2) RAID 1
3) RAID 10
4) RAID 20

5. Если различным группам пользователей с различным уровнем доступа требуется доступ к одной и той же информации, какое из указанных ниже действий следует предпринять руководству?

1) Снизить уровень безопасности этой информации для обеспечения ее доступности и удобства использования
2) Требовать подписания специального разрешения каждый раз, когда человеку требуется доступ к этой информации
3) Улучшить контроль за безопасностью этой информации
4) Снизить уровень классификации этой информации

6. Выберите типы вредоносных программ:

Выберите несколько вариантов ответа:
1) Вирусы, черви, троянские и хакерские программы
2) Шпионское, рекламное программное обеспечение
3) Потенциально опасное программное обеспечение
4) Операционная система Linux
5) Операционная система Windows
6) Microsoft Office

7. Кто является основным ответственным за определение уровня классификации информации?

1) Руководитель среднего звена
2) Высшее руководство
3) Владелец
4) Пользователь

8. Какая категория является наиболее рискованной для компании с точки зрения вероятного мошенничества и нарушения безопасности?

1) Сотрудники
2) Хакеры
3) Атакующие
4) Контрагенты (лица, работающие по договору)

9. Компьютерные вирусы -

1) являются вредоносными программами, которые могут "размножаться" и скрытно внедрять свои копии в файлы, загрузочные секторы дисков и документы. Активизация компьютерного вируса может вызывать уничтожение программ и данных.
2) являются вредоносными программами, которые проникают на компьютер, используя сервисы компьютерных сетей. Их активизация может вызывать уничтожение программ и данных, а также похищение персональных данных пользователя.
3) вредоносная программа, которая выполняет несанкционированную пользователем передачу управления компьютером удалённому пользователю, а также действия по удалению, модификации, сбору и пересылке информации третьим лицам.
4) это программное или аппаратное обеспечение, которое проверяет информацию, входящую в компьютер из локальной сети или Интернета, а затем либо отклоняет её, либо пропускает в компьютер, в зависимости от параметров.
5) программа или набор программ для скрытого взятия под контроль взломанной системы. Это утилиты, используемые для сокрытия вредоносной активности. Они маскируют вредоносные программы, чтобы избежать их обнаружения антивирусными программами.

10. По "среде обитания" вирусы можно разделить на:

Выберите несколько вариантов ответа:
1) загрузочные
2) файловые
3) макровирусы
4) очень опасные
5) не опасные

6) опасные

11. Что самое главное должно продумать руководство при классификации данных?

1) Типы сотрудников, контрагентов и клиентов, которые будут иметь доступ к данным
2) Необходимый уровень доступности, целостности и конфиденциальности
3) Оценить уровень риска и отменить контрмеры
4) Управление доступом, которое должно защищать данные

12. Сетевые черви -

1) являются вредоносными программами, которые могут "размножаться" и скрытно внедрять свои копии в файлы, загрузочные секторы дисков и документы. Активизация компьютерного вируса может вызывать уничтожение программ и данных.
2) являются вредоносными программами, которые проникают на компьютер, используя сервисы компьютерных сетей. Их активизация может вызывать уничтожение программ и данных, а также похищение персональных данных пользователя.
3) вредоносная программа, которая выполняет несанкционированную пользователем передачу управления компьютером удалённому пользователю, а также действия по удалению, модификации, сбору и пересылке информации третьим лицам.
4) это программное или аппаратное обеспечение, которое проверяет информацию, входящую в компьютер из локальной сети или Интернета, а затем либо отклоняет её, либо пропускает в компьютер, в зависимости от параметров.
5) программа или набор программ для скрытого взятия под контроль взломанной системы. Это утилиты, используемые для сокрытия вредоносной активности. Они маскируют вредоносные программы, чтобы избежать их обнаружения антивирусными программами.

13. Сетевые черви бывают:

Выберите несколько вариантов ответа:
1) Web-черви
2) почтовые черви
3) черви операционной системы
4) черви MS Office

14. К биометрическим системам защиты информации относятся системы идентификации по:

Выберите несколько вариантов ответа
1) Отпечатку пальцев
2) Цвету глаз
3) Цвету волос
4) Характеристикам речи
5) Геометрии ладони руки
6) Весу
7) Радужно оболочки глаз
8) Росту
9) Изображению лица

15. Наиболее эффективны от Web-червей, Web-антивирусные программы, которые включают:

Выберите несколько вариантов ответа:
1) межсетевой экран
2) модуль проверки скриптов
3) антивирусный сканер

16. Межсетевой экран (брандмауэр) -

1) являются вредоносными программами, которые могут "размножаться" и скрытно внедрять свои копии в файлы, загрузочные секторы дисков и документы. Активизация компьютерного вируса может вызывать уничтожение программ и данных.
2) являются вредоносными программами, которые проникают на компьютер, используя сервисы компьютерных сетей. Их активизация может вызывать уничтожение программ и данных, а также похищение персональных данных пользователя.
3) вредоносная программа, которая выполняет несанкционированную пользователем передачу управления компьютером удалённому пользователю, а также действия по удалению, модификации, сбору и пересылке информации третьим лицам.
4) это программное или аппаратное обеспечение, которое проверяет информацию, входящую в компьютер из локальной сети или Интернета, а затем либо отклоняет её, либо пропускает в компьютер, в зависимости от параметров.
5) программа или набор программ для скрытого взятия под контроль взломанной системы. Это утилиты, используемые для сокрытия вредоносной активности. Они маскируют вредоносные программы, чтобы избежать их обнаружения антивирусными программами.

17. Троянская программа, троянец -

1) являются вредоносными программами, которые могут "размножаться" и скрытно внедрять свои копии в файлы, загрузочные секторы дисков и документы. Активизация компьютерного вируса может вызывать уничтожение программ и данных.
2) являются вредоносными программами, которые проникают на компьютер, используя сервисы компьютерных сетей. Их активизация может вызывать уничтожение программ и данных, а также похищение персональных данных пользователя.
3) вредоносная программа, которая выполняет несанкционированную пользователем передачу управления компьютером удалённому пользователю, а также действия по удалению, модификации, сбору и пересылке информации третьим лицам.
4) это программное или аппаратное обеспечение, которое проверяет информацию, входящую в компьютер из локальной сети или Интернета, а затем либо отклоняет её, либо пропускает в компьютер, в зависимости от параметров.
5) программа или набор программ для скрытого взятия под контроль взломанной системы. Это утилиты, используемые для сокрытия вредоносной активности. Они маскируют вредоносные программы, чтобы избежать их обнаружения антивирусными программами.

18. Троянские программы бывают:

Выберите несколько вариантов ответа:
1) утилиты удалённого администрирования
2) программы - шпионы
3) рекламные программы
4) программы удаления данных на локальном компьютере

19. От несанкционированного доступа может быть защищен:

1) Каждый диск
2) Файл

3) Ярлык
4) Папка

20. Как классифицируются закладные устройства по способу установки в помещении?

Выберите несколько вариантов ответа
1) с заходом
2) без захода
3) замаскированные
4) незамаскированные.

21. Кто в конечном счете несет ответственность за гарантии того, что данные классифицированы и защищены?

1) Владельцы данных
2) Пользователи
3) Администраторы
4) Руководство

22. Межсетевой экран позволяет:

Выберите несколько вариантов ответа:
1) блокировать хакерские DoS - атаки, не пропуская на защищаемый компьютер сетевые пакеты с определённых серверов
2) не допускать проникновение на защищаемый компьютер сетевых червей
3) препятствовать троянским программам, отправлять конфиденциальную информацию о пользователе и компьютере
4) видеть действия, которые выполняет пользователь на другом компьютере
5) использовать принтер подключённый к другому компьютеру

23. Для защиты от несанкционированного к любым данным, которые хранятся на компьютере, используются:

1) Пароли
2) Логины
3) Коды

24. Как называется биометрическая характеристика, уникальная для каждого человека?

1) Идентификация по ладони руки
2) Идентификация по радужной оболочке глаза
3) Идентификация по изображению лица

25. Если узор … не совпадает с узором допущенного к информации пользователя, то доступ к информации невозможен. Как называется этот критерий?

1) Идентификация по радужной оболочке глаза
2) Идентификация по ладони руки
3) Идентификация по отпечаткам пальцев

26. Руткит - _____ или набор _____ для скрытого взятия под контроль взломанной системы. Это утилиты, используемые для сокрытия вредоносной активности.

Они маскируют вредоносные программы, чтобы избежать их обнаружения антивирусными программами.

27. Коммерческая компания обычно больше заботится о целостности и доступности данных, а военные – о ____*конфиденциальности* _____

28. Не является целью проведения анализа рисков _____ полномочий

29. Выполнение _____ рисков не является здачей руководства в процессе внедрения и сопровождения безопасности

30. Символы шифруемого текста последовательно складываются с символами некоторой специальной последовательности- это метод _____

31. Защита информации – это деятельность по _____ утечки информации, несанкционированных и непреднамеренных воздействий на неё.

32. Антивирус обеспечивает поиск вирусов в оперативной памяти, на внешних носителях путем подсчета и сравнения с эталоном контрольной суммы называется _____

33. Антивирус не только находит зараженные вирусами файлы, но и "лечит" их, т.е. удаляет из файла тело программы вируса, возвращая файлы в исходное состояние называется _____

34. Перехват, который заключается в установке подслушивающего устройства в аппаратуру средств обработки информации называется _____

35. Источник угрозы безопасности информации - субъект (физическое лицо, материальный объект или физическое явление), являющийся непосредственной _____ возникновения угрозы безопасности информации.

36. Защита информации от несанкционированного доступа – защита информации, направленная на _____ получения защищаемой информации заинтересованными субъектами с нарушением установленных нормативными и правовыми документами (актами) или обладателями информации прав или правил разграничения доступа к защищаемой информации.

37. Для защиты от НСД, как правило, используется _____, _____ и управление доступом.

38. Источником угрозы НСД может быть нарушитель, носитель с вредоносной программой или _____.

39. Утечка информации – это неправомерный ___ конфиденциальной информации за пределы защищаемой ____ ее функционирования или установленного круга лиц, результатом которого является получение информации ____, не имеющими к ней санкционированного доступа.

40. Несанкционированный доступ может привести к формам проявления уязвимости информации: ____, _____, искажению, блокированию, ____ и разглашению информации.

41. К утечке информации могут быть причастны лица, как имеющие, так и не имеющие _____ доступ к информации

42. несанкционированный доступ возможен только со стороны лиц, _____ отношения к данной информации по характеру выполняемой работы

43. Канал утечки информации – путь неправомерного ____ информации за пределы защищаемой зоны ее функционирования или установленного круга лиц

44. Технический канал утечки информации – совокупность объекта технической разведки, физической среды распространения информативного сигнала и средств, которыми _____ защищаемая информация

45. Федеральный закон от 27.07.2006 № _____ «Об информации, информационных технологиях и о защите информации»

46. Поиск сигналов является методом перехвата электромагнитных _____ канала несанкционированного доступа к информации

47. Разведка как разведывательная деятельность – это совокупность ___, целенаправленно осуществляемых по добыванию защищаемой информации о вероятном или действительном конкуренте, противнике

48. Промышленный шпионаж добывает информацию по таким вопросам, как издержки, себестоимость, маркетинг, реклама (коммерческий шпионаж), технология (технологический шпионаж), новые ____ и модели продукции (научно-технический шпионаж)

49. Уголовное наказание за совершение преступлений в сфере компьютерной информации предусмотрено главой 28-ой УК РФ. Преступным является неправомерный доступ к охраняемой законом компьютерной информации (ст. _____ УК

50. Персональные данные – данные – любая информация, относящаяся к определенному или определяемому на основании такой информации физическому лицу (субъекту персональных данных), в том числе его ____, год, месяц, дата и ____, адрес, семейное, социальное, имущественное положение, образование, профессия, доходы, другая информация

6 Учебно-методическое и информационное обеспечение дисциплины

6.1 Список источников и литературы

Источники

Основные

1. *Руководящий докумен*т. Защита от несанкционированного доступа к информации. Термины и определения. Утверждено решением председателя Гостехкомиссии России от 30 марта 1992 г. [Электронный ресурс] : Режим доступа : https://fstec.ru/tekhnicheskaya-zashchita-informatsii/dokumenty/114-spetsialnye-normativnye-dokumenty/386-rukovodyashchij-dokument-reshenie-predsedatelya-gostekhkomissii-rossii-ot-30-marta-1992-g3, свободный. – Загл. с экрана.

2. *Руководящий документ*. Автоматизированные системы. Защита от несанкционированного доступа к информации. Классификация автоматизированных

систем и требования по защите информации. Утверждено решением председателя Государственной технической комиссии при Президенте Российской Федерации от 30 марта 1992 г. [Электронный ресурс] : Режим доступа : https://fstec.ru/tekhnicheskaya-zashchita-informatsii/dokumenty/114-spetsialnye-normativnye-dokumenty/384-rukovodyashchij-dokument-reshenie-predsedatelya-gostekhkomissii-rossii-ot-30-marta-1992-g, свободный. – Загл. с экрана.

3. *Руководящий документ*. Средства вычислительной техники. Защита от несанкционированного доступа к информации. Показатели защищённости от несанкционированного доступа к информации. Утверждено решением председателя Государственной технической комиссии при Президенте Российской Федерации от 30 марта 1992 г. [Электронный ресурс]: Режим доступа : https://fstec.ru/tekhnicheskaya-zashchita-informatsii/dokumenty/114-spetsialnye-normativnye-dokumenty/385-rukovodyashchij-dokument-reshenie-predsedatelya-gostekhkomissii-rossii-ot-30-marta-1992-g2, свободный. – Загл. с экрана.

4. *Руководящий документ*. Средства вычислительной техники. Межсетевые экраны Защита от несанкционированного доступа к информации. Показатели защищённости от несанкционированного доступа к информации. Утверждено решением председателя Государственной технической комиссии при Президенте Российской Федерации от 25 июля 1997 г. [Электронный ресурс]: Режим доступа: https://fstec.ru/tekhnicheskaya-zashchita-informatsii/dokumenty/114-spetsialnye-normativnye-dokumenty/383-rukovodyashchij-dokument-reshenie-predsedatelya-gostekhkomissii-rossii-ot-25-iyulya-1997-g, свободный. – Загл. с экрана.

5. *Руководящий документ.* Защита от несанкционированного доступа к информации. Часть 1. Программное обеспечение средств защиты информации. Классификация по уровню контроля отсутствия недекларированных возможностей. Утверждено решением председателя Государственной технической комиссии при Президенте Российской Федерации от 4 июня 1999 г. N 114

6. *Базовая модель угроз* безопасности персональных данных при их обработке в информационных системах персональных данных (выписка). (утв. ФСТЭК РФ 15.02.2008) [Электронный ресурс] : Режим доступа : https://fstec.ru/tekhnicheskaya-zashchita-informatsii/dokumenty/114-spetsialnye-normativnye-dokumenty/379, свободный. – Загл. с экрана.

7. *Федеральный закон* «Об информации, информационных технологиях и о защите информации» от 27.07.2006 N 149-ФЗ (ред. от 19.07.2018). [Электронный ресурс]: Режим доступа: http://www.consultant.ru/document/cons_doc_LAW_61798/, свободный. – Загл. с экрана.

Дополнительные

1. *Приказ ФСТЭК России* от 11.02.2013 № 17 (ред. от 15.02.2017) «Об утверждении Требований о защите информации, не составляющей государственную тайну, содержащейся в государственных информационных системах». [Электронный ресурс]: Режим доступа : http://www.consultant.ru/cons/cgi/online.cgi?req=doc&base=LAW&n=214004&dst=0&rnd=92395C5151F01C02B8725B20C4BBFEB5#034991095371992622 по рабочим дням с 20-00 до 24-00 (время московское), в выходные и праздничные дни в любое время. – Загл. с экрана.

2. *Приказ ФСТЭК России* от 18 февраля 2013 г. № 21. «Об утверждении состава и содержания организационных и технических мер по обеспечению безопасности персональных данных при их обработке в информационных системах персональных данных. [Электронный ресурс]: Режим доступа: http://www.consultant.ru/cons/cgi/online.cgi?

req=doc&base=LAW&n=215976&dst=0&rnd=92395C5151F01C02B8725B20C4BBFEB5#08164959407738432 свободный. – Загл. с экрана.

Литература
Основная
1. Программно-аппаратная защита информации : учеб. пособие / П.Б. Хорев. — 2-е изд., испр. и доп. — Москва : ФОРУМ : ИНФРА-М, 2019. — 352 с. — (Высшее образование). - Текст : электронный. - URL: https://new.znanium.com/catalog/product/1025261

Дополнительная
Система защиты информации от несанкционированного доступа на основе программно-аппаратного комплекса "Secret Net 5.0" / Помешкин А.А., Коротких И.В. - Новосибирск :НГТУ, 2012. - 47 с.: ISBN 978-5-7782-1990-8 - Текст : электронный. - URL: https://new.znanium.com/catalog/product/556699

6.2 Перечень ресурсов информационно-телекоммуникационной сети «Интернет»

1. Банк данных угроз безопасности информации. [Электронный ресурс] / ФСТЭК России, ФАУ «ГНИИИ ПТЗИ ФСТЭК России» – Режим доступа : http://sec.ru/, свободный. – Загл. с экрана.

6.3 Профессиональные базы данных и информационно-справочные системы

Доступ к профессиональным базам данных: https://liber.rsuh.ru/ru/bases

Информационные справочные системы:
1. Консультант Плюс
2. Гарант

7 Материально-техническое обеспечение дисциплины

Для обеспечения дисциплины используется материально-техническая база образовательного учреждения: учебные аудитории, оснащённые доской, а также компьютером и проектором для демонстрации учебных материалов.

Состав программного обеспечения:
Windows
Microsoft Office

8 Обеспечение образовательного процесса для лиц с ограниченными возможностями здоровья и инвалидов

В ходе реализации дисциплины используются следующие дополнительные методы обучения, текущего контроля успеваемости и промежуточной аттестации обучающихся в зависимости от их индивидуальных особенностей:

- для слепых и слабовидящих:

- лекции оформляются в виде электронного документа, доступного с помощью компьютера со специализированным программным обеспечением;

- письменные задания выполняются на компьютере со специализированным программным обеспечением, или могут быть заменены устным ответом;
- обеспечивается индивидуальное равномерное освещение не менее 300 люкс;
- для выполнения задания при необходимости предоставляется увеличивающее устройство; возможно также использование собственных увеличивающих устройств;
- письменные задания оформляются увеличенным шрифтом;
- экзамен и зачёт проводятся в устной форме или выполняются в письменной форме на компьютере.

- для глухих и слабослышащих:

- лекции оформляются в виде электронного документа, либо предоставляется звукоусиливающая аппаратура индивидуального пользования;
- письменные задания выполняются на компьютере в письменной форме;
- экзамен и зачёт проводятся в письменной форме на компьютере; возможно проведение в форме тестирования.

- для лиц с нарушениями опорно-двигательного аппарата:

- лекции оформляются в виде электронного документа, доступного с помощью компьютера со специализированным программным обеспечением;
- письменные задания выполняются на компьютере со специализированным программным обеспечением;
- экзамен и зачёт проводятся в устной форме или выполняются в письменной форме на компьютере.

При необходимости предусматривается увеличение времени для подготовки ответа.

Процедура проведения промежуточной аттестации для обучающихся устанавливается с учётом их индивидуальных психофизических особенностей. Промежуточная аттестация может проводиться в несколько этапов.

При проведении процедуры оценивания результатов обучения предусматривается использование технических средств, необходимых в связи с индивидуальными особенностями обучающихся. Эти средства могут быть предоставлены университетом, или могут использоваться собственные технические средства.

Проведение процедуры оценивания результатов обучения допускается с использованием дистанционных образовательных технологий.

Обеспечивается доступ к информационным и библиографическим ресурсам в сети Интернет для каждого обучающегося в формах, адаптированных к ограничениям их здоровья и восприятия информации:

- для слепых и слабовидящих:

- в печатной форме увеличенным шрифтом;
- в форме электронного документа;
- в форме аудиофайла.

- для глухих и слабослышащих:

- в печатной форме;
- в форме электронного документа.

- для обучающихся с нарушениями опорно-двигательного аппарата:

- в печатной форме;
- в форме электронного документа;
- в форме аудиофайла.

Учебные аудитории для всех видов контактной и самостоятельной работы, научная библиотека и иные помещения для обучения оснащены специальным оборудованием и учебными местами с техническими средствами обучения:

- для слепых и слабовидящих:
  - устройством для сканирования и чтения с камерой SARA CE;
  - дисплеем Брайля PAC Mate 20;
  - принтером Брайля EmBraille ViewPlus;

- для глухих и слабослышащих:

- автоматизированным рабочим местом для людей с нарушением слуха и слабослышащих;
- акустический усилитель и колонки;

- для обучающихся с нарушениями опорно-двигательного аппарата:

- передвижными, регулируемыми эргономическими партами СИ-1;
- компьютерной техникой со специальным программным обеспечением.

9 Методические материалы

9.1 Планы семинарских занятий

Темы учебной дисциплины предусматривают проведение семинарских занятий, которые служат как целям текущего и промежуточного контроля подготовки студентов, так и целям получения навыков практического применения методов выработки решений, закрепления изученного материала, развития умений, приобретения опыта решения конкретных проблем, ведения дискуссий, аргументации и защиты выбранного решения. Помощь в этом оказывают задания, выдаваемые преподавателем на каждом занятии.

Целью семинарских занятий является закрепление теоретического материала и приобретение навыков практической работы с соответствующим оборудованием, программным обеспечением и нормативными правовыми документами.

Тематика семинарских занятий соответствует программе дисциплины.

Результаты семинарских занятий обучающиеся составляют по оговорённой преподавателем форме, в электронном виде с использованием ПКП MS Office 2007 и выше и передаётся преподавателю посредством оговорённого способа связи..

Занятие 1. Система защиту информации от несанкционированного доступа (4 часа)

Задание: Подготовить доклад, сопровождаемый презентацией, по одной из следующих тем:

1. Организация информационной безопасности в гуманитарной сфере.
2. Организация информационной безопасности экономического объекта.
3. Влияние информационного пространства на формирование индивидуального и общественного сознания.

Занятие 2. Защита информации от несанкционированного доступа. Авторизация. Методы идентификации и аутентификации пользователя (4 часа)

Задание: Подготовить доклад, сопровождаемый презентацией, по одной из следующих тем:

1. Биометрические системы аутентификации
2. Многообразие схем авторизации, идентификации и аутентификации пользователя и их сравнительный анализ
3. Управления доступом к информационным ресурсам с помощью «Строгая аутентификация».

Занятие 3. Оценка защищенности информационной среды, разработка методик анализа защищенности системы на основе полученных данных (4 часа)

Задание: Подготовить доклад, сопровождаемый презентацией, по одной из следующих тем:

1. Оценка уровня информационной безопасности
2. Анализ рисков информационной безопасности

3. Разработка методики анализа защищенности информационной системы предприятия.

Занятие 4. Разработка политики безопасности информационной системы (4 часа)

Задание: Подготовить доклад, сопровождаемый презентацией, по одной из следующих тем:
1. Политика безопасности организаций гуманитарной сферы
2. Фрагментарный и комплексный подходы к обеспечению компьютерной безопасности
3. Средства, обеспечивающие информационную безопасность.

Занятие 5. Методика анализа защищённости ИС. Методы и средства выявления угроз её информационной безопасности (4 часа)

Задание: Подготовить доклад, сопровождаемый презентацией, по одной из следующих тем:
1. Организация информационной безопасности в информационном пространстве.
2. Дестабилизирующее воздействие информационных войн на экономику государства
3. Информационный терроризм, методы и средства выявления и противодействия.

Занятие 6. Применение средств аппаратной защиты (4 часа)

Задание: Подготовить доклад, сопровождаемый презентацией, по одной из следующих тем:
1. Аппаратно-программные средства защиты информации
2. Механизмы информационной безопасности: электронная подпись, контроль доступа, дублирование каналов
3. Этапы в жизненном цикле информационного сервиса.

Занятие 7. Комплексный подход при разработке политики безопасности организации (4 часа)

Задание: Подготовить доклад, сопровождаемый презентацией, по одной из следующих тем:
1. Характерные черты функционирования специализированных организаций в сфере информационной безопасности
2. Особенности федерального законодательства по ИБ в РФ
3. Концепция информационной безопасности информационных систем.

Занятие 8. Анализ система мероприятий, направленных на максимальное предотвращение утечки информации (4 часа)

Задание: Подготовить доклад, сопровождаемый презентацией, по одной из следующих тем:
1. Пути и подходы, применяемые для противоправного получения информации, представляющей конкретный интерес для злоумышленников или конкурентов
2. Алгоритм обеспечения информационной безопасности субъектов, связанных с использованием информационных систем
3. Рассмотрение методов обеспечения информационной безопасности в образовательной среде.

Занятие 9. Подходы к оценке эффективности систем информационной безопасности (4 часа)

Задание: Подготовить доклад, сопровождаемый презентацией, по одной из следующих тем:

1. Качественные и количественные аспекты оценки эффективности систем информационной безопасности
2. Оценка экономической эффективности систем информационной безопасности
3. Определение рисков через коэффициенты значимости.

Приложение 1

Аннотация дисциплины (модуля)

Дисциплина «Защита информации от несанкционированного доступа» реализуется на факультете архивоведения и документоведения кафедрой информационной безопасности.

Цель дисциплины – формирование у обучающихся общепрофессиональных и профессиональных компетенций, направленных на приобретение способности инсталлировать программное обеспечение для информационных и автоматизированных систем, способности разрабатывать документы с использованием современных информационных технологий и в условиях современных вызовов.

Задачи:

сформировать знания:

– о современных операционных системах;

– о современном прикладном программном обеспечении для обработки документов и проведении вычислений;

– о сервисных программах операционных систем.

Дисциплина направлена на формирование следующих компетенций:

ПК:

ПК-2 Способен организовать работу с документацией в организациях различных организационно-правовых форм

ПК-4 Способен осуществлять проектирование и внедрение систем электронного документооборота в организации

ОПК:

ОПК-5 Способен самостоятельно работать с различными источниками информации и применять основы информационно-аналитической деятельности при решении профессиональных задач

ОПК-7. Способен к профессиональному росту и самосовершенствованию в области гуманитарных, социальных и лингвистических наук, а также в сфере техники и технологии информатики.

По дисциплине предусмотрена промежуточная аттестация в форме *зачета*.

Общая трудоемкость освоения дисциплины составляет _3_зачетных единицы.