МИНОБРНАУКИ РОССИИ

Федеральное государственное бюджетное образовательное учреждение

высшего образования

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

ИНСТИТУТ ИНФОРМАЦИОННЫХ НАУК И ТЕХНОЛОГИЙ БЕЗОПАСНОСТИ
Факультет информационных систем и безопасности

Кафедра информационной безопасности

ИНФОРМАЦИОННАЯ БЕЗОПАСНОСТЬ АВТОМАТИЗИРОВАННЫХ СИСТЕМ

РАБОЧАЯ ПРОГРАММА ДИСЦИПЛИНЫ

46.04.02 Документоведение и архивоведение с дополнительной квалификацией в области интеллектуальных систем в гуманитарной сфере

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 2024

Информационная безопасность автоматизированных систем
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
№ 9 от 04.04.2024

ОГЛАВЛЕНИЕ

1 Пояснительная записка

1.1 Цель и задачи дисциплины

Цель дисциплины – формирование базовых знаний в области обеспечения информационной безопасности автоматизированных систем (АС); навыков организации работы по оценке эффективности систем безопасности, оптимального выбора и интеграции механизмов обеспечения информационной безопасности.

Задачи дисциплины:

– рассмотрение понятийного базиса в области обеспечения информационной безопасности автоматизированных систем, классов и типовых моделей автоматизированных систем;

– рассмотрение причин нарушения безопасности систем, существа проблемы обеспечения информационной безопасности, концептуальной модели безопасности, формирования требований к безопасности;

– изучение основных механизмов обеспечения информационной безопасности систем;

– изучение безопасного доступа к информационным ресурсам, формирование доверенных сред.

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, имеющиеся ресурсы и ограничения 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-4.3. 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 *«Информационная безопасность автоматизированных систем»* 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 информационную безопасность автоматизированных систем. Понятие и сущность автоматизированных систем. Классификация автоматизированных систем.

Актуальность проблемы защиты АС в современных условиях. Факторы, её определяющие. Защита АС как процесс управления рисками. Анализ рисков. Основные подходы к анализу рисков. Этапы анализа рисков и управления ими. Понятие и сущность автоматизированных систем. Классификация автоматизированных систем.

Методы оценки целесообразности затрат на обеспечение ИБ. Виды затрат на обеспечение ИБ. Особенности современных АС как объектов защиты.

Основные понятия в ИБ АС. Безопасность информации. Информация и её свойства. Цель защиты АС и циркулирующей в ней информации.

Угрозы безопасности АС. Основные структурно-функциональные элементы АС. Типы угроз безопасности. Несанкционированный доступ и несанкционированное воздействие на информацию.

Основные источники угроз безопасности АС. Классификация угроз по источнику возникновения. Критерии классификации и классификация каналов проникновения в АС и утечки информации. Неформальная модель нарушителя. Критерии классификации и

классификация нарушителей.

Тема 2. Организационно-правовые основы обеспечения информационной безопасности автоматизированных систем

Виды мер противодействия угрозам безопасности, их взаимосвязь, достоинства и недостатки. Принципы построения системы обеспечения безопасности информации в АС. Стратегия развития информационного общества в Российской Федерации, утверждённой Президентом РФ от 07.02.2008 № Пр-212. Стратегии национальной безопасности Российской Федерации до 2020 года. Нормативно-методические документы ФСТЭК России по обеспечению безопасности информации. Виды информации по федеральному закону «Об информации, информационных технологиях и о защите информации» от 27.07.2006 № 149-ФЗ.

Понятие лицензии и лицензирования. Виды деятельности в области защиты информации, подлежащих лицензированию. Сертификация средств защиты информации и аттестация объектов информатизации. Термины и определения. Нормативно-правовые акты в области защиты информации от несанкционированного доступа. Классы защиты средств вычислительной техники, АС, межсетевых экранов. Недекларированные возможности. Классификация программного обеспечения по уровню контроля отсутствия в нем недекларированных возможностей.

Тема 3. Автоматизированные системы как объекты обеспечения безопасности информации Угрозы информационной безопасности в АС.

Организационная структура системы обеспечения безопасности АС. Угрозы информационной безопасности в АС Технология управления безопасностью (обеспечения безопасности) информации и ресурсов в АС. Требования к технологии управления безопасностью. Мероприятия при реализации технологии управления безопасностью. Институт ответственных за обеспечение информационной безопасности. Влияние на безопасность ИТ разных субъектов организации ИБ. Цели регламентации действий пользователей и обслуживающего персонала АС. Составляющие эффективного функционирования системы безопасности ИТ. Политика безопасности организации в области ИТ, её цель, условия осуществления и проблемы. Уровни зрелости (в сфере обеспечения ИБ). Виды организационных и организационно-технических мероприятий по созданию и обеспечению функционирования комплексной системы защиты. Распределение функций по обеспечению безопасности АС. Организационно-распорядительные документы по обеспечению безопасности АС. Обязанности пользователей и ответственных за обеспечение ИБ в подразделениях. Проблема человеческого фактора. Общие правила обеспечения безопасности. Обязанности ответственного за обеспечение безопасности информации в подразделении. Ответственность за нарушения требований обеспечения безопасности. Порядок работы с носителями ключевой информации.

Явная и неявная компрометация ключей. Признаки и действия при компрометации ключей. Регламентация правил парольной и антивирусной защиты. Регламентация порядка допуска к работе и изменения полномочий пользователей АС. Регламентация порядка изменения конфигурации аппаратно-программных средств АС.

Тема 4. Средства защиты информации от НСД. Порядок проведения и содержание процедуры расследования компьютерных инцидентов (нарушения ИБ АС).

Способы воздействия на информацию. Причины и условия дестабилизирующего воздействия на информацию. Основные механизмы защиты автоматизированных систем

от НСД. Сущность и назначение идентификации и аутентификации пользователей. Виды и способы аутентификации. Разграничение доступа пользователей к ресурсам АС. Диспетчер доступа. Сущность избирательного и полномочного разграничения доступа. Замкнутая программная среда. Регистрация и оперативное оповещение о событиях безопасности. Криптографические методы защиты информации. Криптография с симметричными и открытыми ключами. Электронная цифровая подпись. Реализация ЭЦП. Принципы комбинированного шифрования. Доверие к открытому ключу и цифровые сертификаты. Система обнаружения атак. Защита периметра компьютерных сетей и управление механизмами защиты.

Аппаратно-программные средства защиты информации от НСД. Рекомендации по выбору СЗИ НСД. Виды биометрической идентификации, преимущества и недостатки.

Применение штатных и дополнительных СЗИ НСД. Стратегия безопасности компании Microsoft. Защита от вмешательства в процесс нормального функционирования АС. Встроенные механизмы разграничения доступа на примере ОС Windows. Уровни доверия механизм целостности. Оперативное оповещение о зарегистрированных попытках НСД. Службы ACS. Система защиты информации от НСД Secret Net 6. Защита данных от несанкционированной модификации, копирования и перехвата средствами шифрования.

Тема 5. Организация комплексной системы защиты информации в АС

Проблемы обеспечения безопасности информации в компьютерных сетях.

Уровни информационной инфраструктуры корпоративной сети. Система разграничения доступа к техническим средствам. Система разграничения доступа к программам и данным. Средства блокировки неправомочных действий субъектов. Уязвимости и их классификация. Типы уязвимости с точки зрения технических особенностей. Классификация уязвимостей по степени риска. Получение информации по уязвимостям. «Стандартные» обозначения уязвимостей. Классификация атак.

Защита периметра корпоративной сети. Угрозы, связанные с периметром корпоративной сети. Составляющие защиты периметра. Межсетевые экраны их виды. Демилитаризованная зона. Анализ содержимого почтового и веб-трафика. Виртуальные частные сети.

Управление уязвимостями. Архитектура систем управления уязвимостями. Особенности сетевых агентов сканирования. Средства анализа защищённости системного уровня. Мониторинг событий безопасности. Категории журналов событий. Инфраструктура управления журналами событий. Особенности защищённости электронного документооборота.

Тема 6. Основы технологии виртуальных защищённых сетей VPN

Концепция построения виртуальных частных сетей – VPN. Основные понятия и функции сети VPN. Защита информации в процессе её передачи по туннелю VPN. VPN-клиент, VPN-сервер и шлюз безопасности VPN. Реализация механизма VPN. Варианты построения виртуальных защищённых каналов. Средства обеспечения безопасности VPN. Критерии безопасности данных применительно к задачам VPN. VPN-решения для построения защищённых сетей. Классификация сетей VPN. Критерии классификации. Основные варианты архитектуры VPN. Достоинства применения технологий VPN.

4 Образовательные технологии

№ п/п	Наименование раздела	Виды учебных занятий	Образовательные технологии

1	2	3	4
1.	Введение в информационную безопасность автоматизированных систем. Понятие и сущность автоматизированных систем. Классификация автоматизированных систем	Лекция Самостоятельная работа	Лекция с использованием видеоматериалов Работа с литературой
2	Организационно-правовые основы обеспечения информационной безопасности автоматизированных систем	Лекция Семинарские занятия Самостоятельная работа	Лекция с использованием видеоматериалов Прием заданий Работа с литературой
3	Автоматизированные системы, как объекты обеспечения безопасности информации. Угрозы информационной безопасности в АС	Лекция Семинарские занятия Самостоятельная работа	Лекция с использованием видеоматериалов Прием заданий Работа с литературой
4	Средства защиты информации от НСД. Порядок проведения и содержание процедуры расследования компьютерных инцидентов (нарушения ИБ АС)	Лекция Семинарские занятия Самостоятельная работа	Лекция с использованием видеоматериалов Прием заданий Работа с литературой
5	Организация комплексной системы защиты информации в АС	Лекция Семинарские занятия Самостоятельная работа	Лекция с использованием видеоматериалов Прием заданий Работа с литературой
6	Основы технологии виртуальных защищённых сетей VPN	Лекция Семинарские занятия Самостоятельная работа	Лекция с использованием видеоматериалов Прием заданий Работа с литературой
7	Аудит информационной безопасности автоматизированных систем	Семинарские занятия Самостоятельная работа	Прием заданий Работа с литературой
8	Автоматизированные системы защиты информации	Семинарские занятия Самостоятельная работа	Прием заданий Работа с литературой
9	Проблемы эксплуатации защищенных автоматизированных систем	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	«удовлетворительно»	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 «Информационная безопасность автоматизированных систем» 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. Актуальность проблемы защиты АС в современных условиях.
2. Защита АС как процесс управления рисками.
3. Методы оценки целесообразности затрат на обеспечение ИБ.
4. Информация и её свойства. Цель защиты АС и циркулирующей в ней информации.
5. Основные структурно-функциональные элементы АС.
6. Типы угроз безопасности. Несанкционированный доступ и несанкционированное воздействие на информацию.
7. Основные источники угроз безопасности АС. Классификация угроз по источнику возникновения.
8. Критерии классификации и классификация каналов проникновения в АС и утечки информации.
9. Неформальная модель нарушителя. Критерии классификации и классификация нарушителей.
10. Виды мер противодействия угрозам безопасности, их взаимосвязь, достоинства и недостатки.
11. Принципы построения системы обеспечения безопасности информации в АС.
12. Понятие лицензии и лицензирования. Виды деятельности в области защиты информации, подлежащих лицензированию. Сертификация средств защиты информации и аттестация объектов информатизации.
13. Нормативно-правовые акты в области защиты информации от несанкционированного доступа. Классы защиты средств вычислительной техники, АС, межсетевых экранов.
14. Недекларированные возможности. Классификация программного обеспечения по уровню контроля отсутствия в нем недекларированных возможностей.
15. Организационная структура системы обеспечения безопасности АС. Институт ответственных за обеспечение информационной безопасности. Влияние на безопасность ИТ разных субъектов организации ИБ.
16. Цели регламентации действий пользователей и обслуживающего персонала АС. Составляющие эффективного функционирования системы безопасности ИТ.
17. Политика безопасности организации в области ИТ, её цель, условия осуществления и проблемы. Уровни зрелости (в сфере обеспечения ИБ.
18. Обязанности пользователей и ответственных за обеспечение ИБ в подразделениях. Проблема человеческого фактора.
19. Порядок работы с носителями ключевой информации. Явная и неявная компрометация ключей.
20. Регламентация правил парольной и антивирусной защиты, порядка допуска к работе и изменения полномочий пользователей АС, порядка изменения конфигурации аппаратно-программных средств АС.
21. Основные механизмы защиты автоматизированных систем от НСД. аутентификации. Разграничение доступа.
22. Криптографические методы защиты информации. Электронная цифровая подпись. Реализация ЭЦП. Принципы комбинированного шифрования.
23. Доверие к открытому ключу и цифровые сертификаты. Система обнаружения атак.
24. Защита периметра компьютерных сетей и управление механизмами защиты.
25. Аппаратно-программные средства защиты информации от НСД. Виды биометрической идентификации, преимущества и недостатки.
26. Применение штатных и дополнительных СЗИ НСД.
27. Уровни информационной инфраструктуры корпоративной сети. Уязвимости и их классификация. Классификация атак.
28. Защита периметра корпоративной сети. Угрозы, связанные с периметром корпоративной сети. Составляющие защиты периметра.

29. Управление уязвимостями. Архитектура систем управления уязвимостями. Особенности сетевых агентов сканирования.
30. Средства анализа защищённости системного уровня. Мониторинг событий безопасности.
31. Системы обнаружения атак. Классификация систем обнаружения атак.
32. Концепция построения виртуальных частных сетей – VPN.
33. Варианты построения виртуальных защищённых каналов.
34. Средства обеспечения безопасности VPN.
35. VPN-решения для построения защищённых сетей. Классификация сетей VPN. Критерии классификации.
36. Основные варианты архитектуры VPN. Достоинства применения технологий VPN.
37. Протоколы формирования защищённых каналов на канальном уровне
38. Протоколы формирования защищённых каналов на сеансовом уровне
39. Защита беспроводных сетей
40. Архитектура средств безопасности IPSec
41. Защита передаваемых данных с помощью протоколов AH и ESP
42. Протокол управления криптоключами IKE
43. Особенности реализации средств IPSec
44. Защита веб-порталов от информационных атак.

Тестовые задания

1) Возможность за приемлемое время получить требуемую информационную услугу называется:
а) Конфиденциальность
б) Доступность
в) Целостность
г) Непрерывность
2) К аспектам информационной безопасности не относится:
а) Доступность
б) Целостность
в) Конфиденциальность
г) Защищенность
3) По каким критериям нельзя классифицировать угрозы:
а) По расположению источника угроз
б) По аспекту информационной безопасности, против которого угрозы направлены в первую очередь
в) По способу предотвращения
г) По компонентам информационных систем, на которые угрозы нацелены
4) Главное достоинство парольной аутентификации – …
а) Простота
б) Надежность
в) Секретность
г) Запоминаемость
5) Сколько уровней включает в себя сетевая модель OSI?
а) 5
б) 7
в) 6
г) 8
6) Межсетевой экран (Брандмауэр, firewall) – это…
а) Комплекс аппаратных средств
б) Комплекс программных средств

в) Комплекс аппаратных или программных средств
г) Комплекс аппаратных и программных средств
7) На каком уровне сетевой модели OSI не работает межсетевой экран:
а) Физический
б) Сеансовый
в) Сетевой
г) Транспортный
8) Межсетевого экрана какого класса не существует:
а) Экранирующий маршрутизатор
б) Экранирующий коммутатор
в) Экранирующий транспорт
г) Экранирующий шлюз
9) Что из перечисленного не входит в состав программного комплекса антивирусной защиты:
а) Подсистема сканирования
б) Подсистема управления
в) Подсистема обнаружения вирусной активности
г) Подсистема устранения вирусной активности
10) На каком этапе заканчивается жизненный цикл автоматизированной системы?
а) Бета-тестирование системы
б) Внедрение финальной версии системы в эксплуатацию
в) Прекращение сопровождения и технической поддержки системы
г) Альфа-тестирование системы
11) Какие задачи выполняет теория защиты информации:
а) Предоставлять полные и адекватные сведения о происхождении, сущности и развитии проблем защиты
б) Аккумулировать опыт предшествующего развития исследований, разработок и практического решения задач защиты информации
в) Формировать научно обоснованные перспективные направления развития теории и практики защиты информации
г) Выполняет все вышеперечисленные
12) Какой из протоколов не относится к протоколам защищенной передачи данных в сети Интернет:
а) SSL
б) SET
в) HTTP
г) IPSec
13) Какого метода разграничения доступа не существует:
а) Разграничение доступа по спискам
б) Разграничение доступа по уровням секретности и категориям
в) Локальное разграничение доступа
г) Парольное разграничение доступа
14) К основным функциям подсистемы защиты операционной системы относятся:
а) Идентификация, аутентификация, авторизация, управление политикой безопасности и разграничение доступа
б) Криптографические функции
в) Сетевые функции
г) Все вышеперечисленные
15) Риск – это…
а) Вероятностная оценка величины возможного ущерба, который может понести владелец информационного ресурса в результате успешно проведенной атаки

б) Фактическая оценка величины ущерба, который понес владелец информационного ресурса в результате успешно проведенной атаки
в) Действие, которое направлено на нарушение конфиденциальности, целостности и/или доступности информации, а также на нелегальное использование других ресурсов сети
г) Реализованная угроза
16) Что из перечисленного не является целью проведения анализа рисков:
а) выявление рисков
б) делегирование полномочий +
в) количественная оценка воздействия потенциальных угроз

17) Эффективная программа безопасности требует сбалансированного применения:
а) контрмер и защитных механизмов
б) процедур безопасности и шифрования
в) технических и нетехнических методов
18) Какая из приведенных техник является самой важной при выборе конкретных защитных мер:
а) анализ рисков
б) результаты ALE
в) анализ затрат / выгоды
19) Кто в конечном счете несет ответственность за гарантии того, что данные классифицированы и защищены:
а) владельцы данных
б) руководство
в) администраторы
20) Какая категория является наиболее рискованной для компании с точки зрения вероятного мошенничества и нарушения безопасности:
а) хакеры
б) контрагенты
в) сотрудники
21) Информационная безопасность автоматизированных систем зависит от:
а) компьютеров, поддерживающей инфраструктуры
б) пользователей
в) информации
22) Под информационной безопасностью понимается:
а) защищенность информации и поддерживающей инфраструктуры от случайных или преднамеренных воздействий естественного или случайного характера, которые могут нанести неприемлемый ущерб субъектам информационных отношений в том числе владельцам и пользователям информации и поддерживающей инфраструктуре
б) программный продукт и базы данных должны быть защищены по нескольким направлениям от воздействия
в) нет верного ответа
23) Таргетированная атака — это:
а) атака на сетевое оборудование
б) атака на компьютерную систему крупного предприятия
в) атака на конкретный компьютер пользователя
24) Какие вирусы активизируются в самом начале работы с операционной системой:
а) загрузочные вирусы
в) троянцы
г) черви
25) Диспетчер доступа – это:

а) средство, выступающее в роли посредника-контролёра при обращении субъектов доступа к объектам доступа
б) средство, осуществляющее мандатный доступ субъектов доступа к объектам доступа
в) средство, осуществляющее дискреционный доступ субъектов доступа к объектам доступа

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

27. Выполнение _____ рисков не является задачей руководства в процессе внедрения и сопровождения безопасности

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

29. Какие _____ вирусы активизируются в самом начале работы с операционной системой:

30. Доктрина информационной безопасности РФ – это совокупность официальных взглядов на цели, задачи, принципы и основные направления обеспечения _____ РФ

31. К недостаткам аппаратных средств инженерно-технической защиты относят _____ гибкость

32. Накопление _____ об угрозах информационной безопасности и их аналитическая обработка относятся к выявлению гроз

33. Основной и трудно контролируемый канал утечки информации, составляющей коммерческую тайну – это _____ специалистов

34. Перечень сведений, доступ к которым не может быть ограничен, определен Федеральным законом от 27 июля 2006 г.№ _____

35. Перечень сведений конфиденциального характера определен Указом _____ от 6 марта 1997 г. № 188

36. Радиоволны _____ диапазона распространяются на расстояние прямой видимости в пределах единиц и десятков километров

37. Основной целью обеспечения информационной безопасности автоматизированной системы является защита участников информационного взаимодействия от ущерба, который они могут понести в результате вмешательства в работу системы, а также _____ на саму информацию или отдельные компоненты АС.

38. Межсетевой экран выполняет функцию разграничения информационных потоков на границе _____ автоматизированной системы

39. DLP системы предназначены для предотвращения несанкционированной передачи защищаемой информации за _____ автоматизированной системы

40. Организация надлежащего исполнения правил эксплуатации средств криптографической ЗИ (в том числе во время приемочных испытаний) возлагается на _____ организаций, эксплуатирующих
данные средства.

41. Аттестация автоматизированных средств защиты информации проводится _____ автоматизированных средств защиты информации в постоянную эксплуатацию в соответствии с положениями нормативных правовых актов и методических документов уполномоченных федеральных органов исполнительной власти и национальных стандартов

42. Формирование требований к системе защиты информации автоматизированных средств защиты информации определяется ГОСТ _____

43. Основными административными методами обеспечения информационной безопасности АС являются: утверждение на предприятии _____ нормативных актов, регламентирующих доступ к АС, защиту и обработку данных; _____ и мотивация сотрудников; введение режима коммерческой тайны и _____ за ее разглашение, внесение соответствующих положений в трудовые _____; формирование у работников заинтересованности в защите данных.

44. Принципиальное отличие межсетевых экранов (МЭ) от систем обнаружения атак (СОВ) заключается в том, что МЭ были разработаны для активной или пассивной _____, а СОВ – для активного или пассивного _____.

45. Информация, составляющая государственную тайну не может иметь гриф ____

46. В статье 274 УК РФ определена ответственность за нарушение правил эксплуатации ____, системы ЭВМ или их сети.

47. Возглавляет государственные органы обеспечения информационной безопасности _____

48. Помехоустойчивое кодирование при создании отказоустойчивых систем, как правило, используется в _____ с другими подходами повышения отказоустойчивости

49. Принцип действия емкостных датчиков заключается в ____ эквивалентной емкости в контуре генератора сигналов датчика, которое вызывается увеличением распределенной емкости между злоумышленником и антенной датчика.

50. Под скремблированием понимается изменение характеристик речевого сигнала таким образом, что полученный _____ сигнал, обладая свойствами неразборчивости и неузнаваемости, занимает такую же полосу частот спектра, как и исходный открытый

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. *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.

3. Уголовный кодекс Российской Федерации от 13.06.1996 № 63-ФЗ (ред. от 03.07.2018). [Электронный ресурс] : Режим доступа : http://www.consultant.ru/document/cons_doc_ LAW_10699/, свободный. – Загл. с экрана.

Литература

Основная

1. Комплексная защита информации в корпоративных системах : учеб. пособие / В.Ф. Шаньгин. – Москва : ИД «ФОРУМ» : ИНФРА-М, 2019. – 592 с. – (Высшее образование: Бакалавриат). – Текст : электронный. – URL: https://new.znanium.com/catalog/product/996789
2. 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

1. Модель нарушителя прав доступа в автоматизированной системе [Программные продукты и системы, №2 (98), 2012, стр. -] - Текст : электронный. - URL: https://new.znanium.com/catalog/product/470655

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.
2. OXPAHA.ru. Российское СМИ о безопасности. [Электронный ресурс]: Режим доступа : https://oxpaha.ru/, свободный. – Загл. с экрана.
3. Sec.ru. Портал по безопасности. [Электронный ресурс]: Режим доступа: http://sec.ru/, необходима регистрация. – 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:

1. Windows
2. 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. Понятие и сущность автоматизированных систем. Классификация автоматизированных систем (4 часа)

Задание:

Теоретическая часть

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

1. Компоненты автоматизированной системы и их функционал.
2. Роль человека в обеспечении функционала автоматизированной системы.
3. Влияние информационного пространства на формирование индивидуального и общественного сознания.

Практическая часть

1. Разработать для предложенной фирмы виды организационных и организационно-технических мероприятий по созданию и обеспечению функционирования комплексной системы защиты.

Указания по выполнению заданий:

1. Изучить теоретические материалы.
2. Преподаватель выдаёт каждому перечень объектов автоматизированной системы, структуру и штат организации.

Отчет должен содержать:

- наименование работы;
- цель работы;
- задание;

- последовательность выполнения работы;
- ответы на контрольные вопросы;
- вывод о проделанной работе

Занятие 2. Организационно-правовые основы обеспечения информационной безопасности автоматизированных систем (4 часа)

Задание:

Теоретическая часть

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

1. Административно-правовое и гражданско-правовое обеспечение информационной безопасности автоматизированных систем
2. Уголовно-правовое обеспечение информационной безопасности автоматизированных систем
3. Материальная ответственность при обеспечении информационной безопасности автоматизированных систем

Практическая часть

1. Разработать систему защиты периметра сети организации.
2. Спроектировать демилитаризованную зону с указанием оборудования вынесенного в ДМЗ.

Указания по выполнению заданий:

1. Преподаватель выдаёт каждому перечень объектов автоматизированной системы, структуру и штат организации.

Отчет должен содержать:

- наименование работы;
- цель работы;
- задание;
- последовательность выполнения работы;
- ответы на контрольные вопросы;
- вывод о проделанной работе

Занятие 3. Автоматизированные системы как объекты обеспечения безопасности информации Угрозы информационной безопасности в АС (4 часа)

Задание:

Теоретическая часть

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

1. Содержание работ по созданию автоматизированной системы в защищенном исполнении
2. Содержание и порядок выполнения работ на стадиях и этапах создания автоматизированных систем
3. Угрозы информационной безопасности в АС

Практическая часть

1. Составить матрицу разделения доступа к ресурсам для предложенной фирмы.
2. Выполнить мандатное разграничение доступа к ресурсам.
3. Выбрать модель разграничения доступа.

Указания по выполнению заданий:

1. Преподаватель выдаёт каждому перечень объектов автоматизированной системы, структуру и штат организации.

Занятие 4. Средства защиты информации от НСД. Порядок проведения и содержание процедуры расследования компьютерных инцидентов (4 часа)

Задание:

Теоретическая часть

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

1. Средства защиты информации от НСД. Понятия компьютерного преступления и инцидента информационной безопасности
2. Классификация правонарушений в компьютерной сфере. Первичное реагирование на инцидент ИБ
3. Методы и средства исследования компьютерных систем.

Практическая часть

1. Сформировать в симуляторе Cisco Packet Tracer по заданной топологии сеть (задать адреса узлов шлюзов)
2. Создать безопасный удалённый доступ (SSH) к указанному узлу.
3. Изучить прохождение пакетов, оформить отчёт.
4. Ответить на контрольные вопросы

Указания по выполнению заданий:

1. Изучить теоретический материал по теме.
2. Преподаватель выдаёт каждому студенту адресное пространство сети класса С.

Занятие 5. Организация комплексной системы защиты информации в АС (4 часа)

Задание:

Теоретическая часть

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

1. Технологическое и организационное построение комплексной системы защиты информации.
2. Кадровое обеспечение функционирования комплексной системы защиты информации
3. Материально-техническое и нормативно-методическое обеспечение функционирования комплексной системы защиты информации.

Практическая часть

Разработка набора типовых вариантов комплексных средств защиты информации применительно к объекту защиты

Указания по выполнению заданий:

1. Изучить теоретические материалы.
2. Преподаватель выдаёт каждому объект автоматизированной системы, структуру и штат организации.

Отчет должен содержать:

- наименование работы;
- цель работы;
- задание;
- последовательность выполнения работы;
- вывод о проделанной работе

Занятие 6. Основы технологии виртуальных защищённых сетей VPN (4 часа)

Задание:

Теоретическая часть

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

1. Основы туннелирования и протоколирования
2. Перспективы VPN
3. VPN на базе брандмауэра и программного обеспечения.

Практическая часть

1. Разработать систему VPN для организации.

Указания по выполнению заданий:

1. Преподаватель выдаёт каждому перечень объектов автоматизированной системы, структуру и штат организации.

Занятие 7. Аудит информационной безопасности автоматизированных систем (4 часа)

Задание:

Теоретическая часть

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

1. Содержание аудита безопасности и перечень исходных данных, необходимых для проведения аудита
2. Требования к аккредитации компаний, занимающихся аудитом информационной безопасности
3. Подготовка и содержание отчета по результатам аудита.

Практическая часть

Необходимо создать протокол оценки эффективности, установленных на объекте средств защиты информации для выбранной организации (выдается преподавателем).

Отчет должен содержать: протокол оценки эффективности, установленных на объекте средств защиты информации для конкретной организации.

Занятие 8. Автоматизированные системы защиты информации (4 часа)

Задание:

Теоретическая часть

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

1. Создание автоматизированных систем в защищенном исполнении
2. Внедрение системы защиты информации автоматизированных систем защиты информации
3. Базовые подсистемы защиты информации в составе объекта информатизации.

Практическая часть

Объект оценки представляет собой помещение из трех комнат: приемная, рабочая комната основного персонала и кабинет директора. Организация, расположенная в данном помещении, занимается закупкой печатной и канцелярской продукции у производителя и последующим распространением по книжным магазинам. Следовательно, возникает проблема защиты коммерческой и служебной информации.

Для обработки защищаемой информации используется 7 компьютеров, 6 из которых расположены в помещении без окон. Вся конфиденциальная информация хранится на сервере, находящемся в закрытом серверном шкафу. Есть телефон, сотрудники имеют возможность переговариваться в процессе работы и совершать внешние звонки. Сеть основана на экранированной витой паре, что исключает возможность снятия информации с кабеля. Сеть имеет доступ в Интернет через прокси-сервер. Защита внутренней сети реализована аппаратно посредством межсетевого экрана маршрутизатора и программно посредством межсетевого экрана, установленного на прокси-сервере. Все конфиденциальные переговоры ведутся в помещении без окон.

- Описать структуру предприятия.
- Составить перечень объектов защиты организации.

- Определить и описать полное множество угроз информационной безопасности для анализа организации.
- Заполнить базу данных для рассматриваемого варианта (угрозы, объекты защиты).
- Сформулировать выводы.
- Описать предполагаемые средства защиты на рассматриваемом объекте.

Занятие 9. Проблемы эксплуатации защищенных автоматизированных систем (4 часа)

Задание:

Теоретическая часть

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

1. Особенности защиты информации при использовании съемных накопителей информации большой емкости
2. Проблемы эксплуатации автоматизированных систем при межсетевом взаимодействии
3. Проблемы, возникающие при аттестации автоматизированных систем.

Практическая часть

Опишите возможные сбои/отказы компонентов систем защиты информации и пути решения проблем. Разработайте план обеспечения непрерывной работы и восстановления работоспособности подсистемы защиты информации автоматизированной системы.

Отчет должен содержать:

- наименование работы;
- цель работы;
- задание;
- последовательность выполнения работы;
- вывод о проделанной работе

Приложение 1

Аннотация дисциплины (модуля)

Дисциплина «Информационная безопасность автоматизированных систем» реализуется на факультете архивоведения и документоведения кафедрой информационной безопасности.

Цель дисциплины – формирование базовых знаний в области обеспечения информационной безопасности автоматизированных систем; навыков организации работы по оценке эффективности систем безопасности, оптимального выбора и интеграции механизмов обеспечения информационной безопасности.

Задачи:

– рассмотрение понятийного базиса в области обеспечения информационной безопасности автоматизированных систем, классов и типовых моделей автоматизированных систем;

– рассмотрение причин нарушения безопасности систем, существа проблемы обеспечения информационной безопасности, концептуальной модели безопасности, формирования требований к безопасности;

– изучение основных механизмов обеспечения информационной безопасности систем;

– изучение безопасного доступа к информационным ресурсам, формирование доверенных сред.

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.

По дисциплине предусмотрена промежуточная аттестация в форме *зачета*.

Общая трудоемкость освоения дисциплины составляет _3_зачетных единицы.