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 комплексной защиты информации

ЗАЩИЩЕННЫЕ ИНФОРМАЦИОННЫЕ СИСТЕМЫ

РАБОЧАЯ ПРОГРАММА ДИСЦИПЛИНЫ

10.04.01 Информационная безопасность
Код и наименование направления подготовки

Организация и технологии защиты государственной тайны
Наименование направленности (профиля)

Уровень высшего образования: *магистратура*

Форма обучения: *очная*

РПД адаптирована для лиц
с ограниченными возможностями
здоровья и инвалидов

Москва 2022

Защищённые информационные системы
Рабочая программа дисциплины
Составитель:
Кандидат технических наук, доцент кафедры комплексной защиты информации
А.С. Моляков

Ответственный редактор
Кандидат технических наук, и.о. зав. кафедрой комплексной защиты информации
Д.А. Митюшин

УТВЕРЖДЕНО
Протокол заседания кафедры КЗИ
№ 8 от 31.03.2022

ОГЛАВЛЕНИЕ

1. Пояснительная записка

1.1. Цель и задачи дисциплины

Цель дисциплины – профессиональная подготовка магистрантов, необходимая для освоения методов и технологий защиты информационных систем.

Задачи дисциплины: освоение основных понятий и терминологии, технологий и навыков настройки и эксплуатации защищённых информационных систем, изучение нормативных правовых актов в области защищённых информационных систем, архитектуры защищённых информационных систем.

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

Компетенция (код и наименование)	**Индикаторы компетенций** (код и наименование)	**Результаты обучения**
УК-4 – Способен применять современные коммуникативные технологии, в том числе на иностранном(ых) языке(ах), для академического и профессионального взаимодействия	УК-4.1 – Знает современные коммуникативные технологии на государственном и иностранном языках; закономерности деловой устной и письменной коммуникации	*Знать:* • современные коммуникативные технологии на государственном и иностранном языках; • закономерности деловой устной и письменной коммуникации
	УК-4.2 – Умеет применять на практике коммуникативные технологии, методы и способы делового общения	*Уметь:* • применять на практике коммуникативные технологии, методы и способы делового общения
	УК-4.3 – Владеет методикой межличностного делового общения на государственном и иностранном языках, с применением профессиональных языковых форм и средств	*Владеть:* • методикой межличностного делового общения на государственном и иностранном языках, с применением профессиональных языковых форм и средств
ОПК-1 – Способен обосновывать требования к системе обеспечения информационной безопасности и разрабатывать проект технического задания на ее создание	ОПК-1.1 – Знает основы отечественных и зарубежных стандартов в области обеспечения информационной безопасности	*Знать:* • основы отечественных и зарубежных стандартов в области обеспечения информационной безопасности
	ОПК-1.2 – Умеет проектировать информационные системы с учётом различных технологий обеспечения информационной безопасности	*Уметь:* • проектировать информационные системы с учётом различных технологий обеспечения информационной безопасности

	ОПК-1.3 – Владеет навыками участия в разработке системы обеспечения информационной безопасности объекта	*Владеть:* • навыками участия в разработке системы обеспечения информационной безопасности объекта языковых форм и средств
ОПК-2 – Способен разрабатывать технический проект системы (подсистемы либо компонента системы) обеспечения информационной безопасности	ОПК-2.1 – Знает методы концептуального проектирования технологий обеспечения информационной безопасности	*Знать:* • методы концептуального проектирования технологий обеспечения информационной безопасности
	ОПК-2.2 – Умеет выбирать и обосновывать преимущества методов решения задач для защиты информации компьютерных систем и сетей и систем обеспечения информационной безопасности	*Уметь:* • выбирать и обосновывать преимущества методов решения задач для защиты информации компьютерных систем и сетей и систем обеспечения информационной безопасности
	ОПК-2.3 – Владеет навыками выполнения работы по осуществлению при изготовлении, монтаже, наладке, испытаниях и сдаче в эксплуатацию систем и средств обеспечения информационной безопасности	*Владеть:* • навыками выполнения работы по осуществлению при изготовлении, монтаже, наладке, испытаниях и сдаче в эксплуатацию систем и средств обеспечения информационной безопасности

1.3. Место дисциплины в структуре образовательной программы

Дисциплина «Защищённые информационные системы» относится к обязательной части блока дисциплин учебного плана.

Для освоения дисциплины необходимы знания, умения и владения, сформированные в ходе изучения следующих дисциплин и прохождения практик: дисциплина является дисциплиной начального цикла обучения.

В результате освоения дисциплины формируются знания, умения и владения, необходимые для изучения следующих дисциплин и прохождения практик: «Теоретические аспекты безопасности компьютерных систем », «Типовые подсистемы и решения обеспечения информационной безопасности», «Проектно-технологическая практика» и «Преддипломная практика».

2. Структура дисциплины

Общая трудоёмкость дисциплины составляет 5 з.е., 180 академических часов.

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
1	Лекции	36
1	Практические работы	44
	Всего:	80

Объем дисциплины (модуля) в форме самостоятельной работы обучающихся составляет 82 академических часа.

3. Содержание дисциплины

№	Наименование раздела дисциплины	Содержание
1	**Основные понятия защищённых информационных систем. Общие принципы построения защищённых информационных систем**	Понятие «информационная система». Концепция безопасности информационной системы. Цели обеспечения информационной безопасности. Санкционированный и несанкционированный доступ. Угрозы безопасности и каналы реализации угроз. Уровни защиты информации. Стандарты безопасности. Классы защищённости информационных систем. Нормативная база Российской Федерации и иностранных государств. Современная доктрина информационной безопасности Российской Федерации.
2	**Архитектура информационных систем на основе баз данных. Технологии проектирования баз данных**	Трёхуровневая архитектура информационных систем на основе баз данных. Модели данных. Структура данных. Целостность реляционных данных. Основные этапы проектирования баз данных. Технологии проектирования на основе нормализации. Технологии проектирования на основе модели «Сущность-связь».
3	**Разграничения доступа к ресурсам информационной системы**	Основные понятия систем разграничения доступа. Сущность и определение политики безопасности. Основные типы политик безопасности: мандатные, ролевые, контроля целостности информационных ресурсов, избирательного разграничения доступа. Субъектно-объектная модель информационной системы.

4	**Средства обеспечения целостности информационных систем на основе баз данных. Средства обеспечения конфиденциальности информации в системах на основе баз данных**	Угрозы целостности информации. Способы противодействия. Понятие и основные свойства транзакций. Механизм блокировок. Декларативная и процедурная ссылочные целостности. Способы поддержания ссылочной целостности. Триггеры и правила. Угрозы конфиденциальности информации. Средства идентификации и аутентификации в СУБД. Средства управления доступом. Виды привилегий. Использование механизма ролей. Метки безопасности. Использование представлений для обеспечения конфиденциальности информации.
5	**Способы хранения конфиденциальной информации**	Положение о конфиденциальной информации в электронном виде. Контентная категоризация. Классификация информации по уровню конфиденциальности. Метки документов. Способы хранение конфиденциальной информации. Сводная информация. Интеллектуальная собственность. Неструктурированная информация.
6	**Основные направления защиты информации. Организационные меры защиты информации в организации**	Защита документов. Защита каналов утечки конфиденциальной информации. Мониторинг действий пользователей. Классификация внутренних нарушителей: неосторожные, манипулируемые, саботажники, нелояльные, мотивированные извне. Другие градации. Кадровая политика. Определение прав локальных пользователей. Стандартизация программного обеспечения. Организация процедуры хранения физических носителей информации. Определение уровней контроля информационных потоков. Режимы архива, сигнализации, активной защиты.
7	**Классификация межсетевых экранов. Их политики. Типы окружений межсетевых экранов. Политика безопасности межсетевых экранов**	Классификация. Установление TCP-соединения. Пакетные фильтры, набор правил. Пограничные маршрутизаторы. Межсетевые экраны (МЭ) на основе технологий Stateful Inspection и Host-based. Персональные МЭ и их персональные устройства. Прокси-сервер прикладного уровня. Выделенные прокси-серверы. Гибридные технологии МЭ. Трансляция сетевых адресов (NAT). Статическая и скрытая трансляция NAT. Принцип построения окружения МЭ. DMZ-сети. Конфигурация с одной DMZ-сетью. Service Leg конфигурация. Конфигурация с двумя DMZ-сетями. Виртуальные частные сети.

		Расположение VPN-серверов. Интранет. Экстранет. Компоненты инфраструктуры: концентраторы и коммутаторы. Расположение серверов в DMZ-сетях. Внешне доступные серверы. VPN и Dial-in серверы. Внутренние серверы. DNS-серверы. SMTP-серверы. Политика МЭ. Реализация его набора правил. Тестирование политики МЭ. Возможные подходы к эксплуатации МЭ а. Сопровождение МЭ и управление им. Физическая безопасность окружения МЭ. Администрирование МЭ. Стратегия восстановления после сбоев. Возможность создания логов МЭ. Инциденты безопасности.
8	**Системы обнаружения атак**	Понятие системы обнаружения атак (IDS). Типы и базовая структура IDS. Совместное расположение Host и Target. Разделение Host и управления. Полностью распределённое управление. Network-based IDS, Host-based IDS, Application-based IDS. Анализ, выполняемый IDS. Определение злоупотреблений. Активные и пассивные ответные действия. Использование SNMP TRAPS. Системы анализа и оценки уязвимостей. Host-based и Network-based анализ уязвимостей. Способы взаимодействия сканера уязвимостей и IDS.
9	**Безопасное использование службы доменных имён (DNS)**	Безопасность DNS. Сервисы DNS. Инфраструктура DNS. Компоненты DNS и понятие безопасности. Основные механизмы безопасности для сервисов DNS. Данные DNS и ПО DNS. Name-серверы, Авторитетные и кэширующие Name-серверы. Resolver′ы. Транзакции DNS. Запрос/ответ DNS. Зонная пересылка. Динамические обновления. Безопасность окружения DNS. Угрозы для ПО и данных DNS.
10	**Обеспечение безопасности WEB-серверов. Безопасность WEB-ориентированного контента**	Причины уязвимости WEB-сервера. Планирование развёртывания WEB-сервера. Безопасное инсталлирование и конфигурирование используемой ОС. Удаление или запрещение ненужных сервисов и приложений. Управление ресурсами на уровне ОС. Альтернативные платформы для WEB-сервера. Использование Appliances для WEB-сервера. Специально усиленные ОС и WEB-серверы. Тестирование безопасности ОС.Безопасное инсталлирование и конфигурирование WEB-сервера. Соответствующий список действий. Разграничение доступа для ПО WEB-сервера.

		Управление доступом к директории содержимого WEB-сервера. Публикации информации на WEB-сайтах. Обеспечение безопасности технологий создания активного содержимого. URLs и cookies. Уязвимости технологий активного содержимого на стороне клиента. Уязвимости технологий создания содержимого на стороне сервера. Необходимые действия для обеспечения безопасности WEB-содержимого.
11	**Технологии аутентификации и шифрования**	Требования к аутентификации и шифрованию. Аутентификация, основанная на IP-адресе. Basic и Digest аутентификации. SSL/TLS. Возможности и слабые места SSL/TLS. Пример SSL/TLS сессии. Схемы шифрования SSL/TLS. Список действий при использовании технологий аутентификации и шифрования. Wirewall прикладного уровня для Web: ModSecurity.

4. Образовательные технологии

№ п/п	Наименование раздела	Виды учебных занятий	Образовательные технологии
1	**2**	**3**	**4**
1.	Основные понятия защищённых информационных систем. Общие принципы построения защищённых информационных систем.	Лекция 1.1 Лекция 1.2 Самостоятельная работа	Традиционная лекция с использованием презентаций Опрос Работа с литературой Консультирование и проверка заданий посредством электронной почты
2	Архитектура информационных систем на основе баз данных. Технологии проектирования баз данных.	Лекция 2.1 Лекция 2.2 Самостоятельная работа	Традиционная лекция с использованием презентаций Опрос Работа с литературой Консультирование и проверка заданий посредством электронной почты
3	Разграничения доступа к ресурсам информационной системы	Лекция 3.1 Лекция 3.2 Самостоятельная работа	Традиционная лекция с использованием презентаций Опрос Работа с литературой Консультирование и проверка заданий посредством электронной почты

4	Средства обеспечения целостности информационных систем на основе баз данных. Средства обеспечения конфиденциальности информации в системах на основе баз данных.	Лекция 4.1 Лекция 4.2 Лекция 4.3 Практическое занятие 1. Самостоятельная работа	Традиционная лекция с использованием презентаций Опрос Выполнение задания Работа с литературой Консультирование и проверка заданий посредством электронной почты
5	Способы хранения конфиденциальной информации	Лекция 5.1 Лекция 5.2 Самостоятельная работа	Традиционная лекция с использованием презентаций Опрос Работа с литературой Консультирование и проверка заданий посредством электронной почты
6	Основные направления защиты информации. Организационные меры защиты информации в организации	Лекция 6.1 Лекция 6.2 Практическое занятие 2. Самостоятельная работа	Традиционная лекция с использованием презентаций Опрос Выполнение задания Работа с литературой Консультирование и проверка заданий посредством электронной почты
7	Классификация межсетевых экранов. Их политики. Типы окружений межсетевых экранов. Политика безопасности межсетевых экранов.	Лекция 7.1 Лекция 7.2 Лекция 7.3 Практическое занятие 3. Самостоятельная работа	Традиционная лекция с использованием презентаций Опрос Выполнение задания Работа с литературой Консультирование и проверка заданий посредством
8	Системы обнаружения атак.	Лекция 8.1 Лекция 8.2 Самостоятельная работа	Традиционная лекция с использованием презентаций Опрос Работа с литературой Консультирование и проверка заданий посредством электронной почты
9	Безопасное использование службы доменных имён (DNS)	Лекция 9.1 Лекция 9.2 Практическое занятие 4. Самостоятельная работа	Традиционная лекция с использованием презентаций Опрос Выполнение задания Работа с литературой

			Консультирование и проверка заданий посредством электронной почты
10	Обеспечение безопасности WEB-серверов. Безопасность WEB-ориентированного контента.	Лекция 10.1 Лекция 10.2 Практическое занятие 5. Самостоятельная работа	Традиционная лекция с использованием презентаций Опрос Выполнение задания Работа с литературой Консультирование и проверка заданий посредством электронной почты
11	Технологии аутентификации и шифрования.	Лекция 11.1 Лекция 11.2 Практическое занятие 6. Самостоятельная работа	Традиционная лекция с использованием презентаций Опрос Выполнение задания Работа с литературой Консультирование и проверка заданий посредством электронной почты

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 или тестирование (темы 1-11)	*2 балла*	*22 балла*
- практические занятия 1-5	*6 баллов*	*30 баллов*
- практическое занятие 6	*8 баллов*	*8 баллов*
Промежуточная аттестация - *экзамен*		40 баллов
Итого за семестр		100 баллов

5.2. Критерии выставления оценки по дисциплине

Баллы/ Шкала ECTS	**Оценка по дисциплине**	**Критерии оценки результатов обучения по дисциплине**
100-83/ A,B	«отлично»/ «зачтено (отлично)»/ «зачтено»	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»/ «зачтено (хорошо)»/ «зачтено»	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»/ «зачтено (удовлетвори-тельно)»/ «зачтено»	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. Оценка по дисциплине выставляются обучающемуся с

Баллы/ Шкала ECTS	Оценка по дисциплине	Критерии оценки результатов обучения по дисциплине
		учётом результатов текущей и промежуточной аттестации. Компетенции, закреплённые за дисциплиной, сформированы на уровне – «достаточный».
49-0/ F,FX	«неудовлетворительно»/ не зачтено	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

Устный опрос

Устный опрос – это средство контроля, организованное как специальная беседа преподавателя с обучающимся на темы, связанные с изучаемой дисциплиной, и рассчитанное на выяснение объёма знаний, обучающегося по определённому разделу, теме, проблеме и т.п.

Перечень устных вопросов для проверки знаний

№	Вопрос
1.	Что такое информационная система?
2.	Основные положения Доктрины информационной безопасности Российской Федерации
3.	Основные понятия систем разграничения доступа
4.	Сущность и определение политики безопасности.
5.	Основные типы политик безопасности
6.	Понятие и основные свойства транзакций
7.	Межсетевые экраны их виды. Администрирование межсетевых экранов.
8.	Демилитаризованная зона, её понятие и структура
9.	Составляющие защиты периметра.
10.	Особенности периметра современных КС
11.	Реализация механизма VPN
12.	VPN-клиент, VPN-сервер и шлюз безопасности VPN.
13.	Классификация сетей VPN.
14.	Протокол PPTP. Структура пакета.

15.	Процедура установления SSL-сессии.
16.	Защита беспроводных сетей
17.	Архитектура стека протоколов IPSec
18.	Защита передаваемых данных с помощью протоколов AH и ESP
19.	Протокол аутентифицирующего заголовка.
20.	Применение протокола AH в транспортном и туннельном режимах
21.	Протокол инкапсулирующей защиты, применение протокола ESP в транспортном и туннельном режимах.
22.	Протокол управления криптоключами IKE
23.	Задачи, решаемые протоколами IKE
24.	Практические аспекты защиты веб-порталов от информационных атак
25.	Типовая архитектура веб-портала
26.	Подсистемы антивирусной защиты
27.	Подсистемы контроля целостности
28.	Подсистемы разграничения доступа
29.	Подсистемы обнаружения вторжений
30.	Сервисы DNS
31.	Основные механизмы безопасности для сервисов DNS
32.	Причины уязвимости WEB-сервера

Примерные тестовые задания

(проверка сформированности компетенций – УК-4)

1. Чем преимущественно мыслят деловые партнеры с визуальной модальностью? Приведите две позиции.

2. Что относится к открытым вопросам в деловой коммуникации?

3. Приведите пример одного из первичных признаков, которые свидетельствуют о наличии манипуляции в деловом общении.

4. Расставьте в правильной последовательности в порядке убывания значимости определения классов защищенности ИСПДн (Информационных систем персональных данных) при проведении аттестации в соответствии с Приказом ФСТЭК России № 21 от 18 февраля 2013 г.

a) К-3
b) К-4
c) К-1
d) К-2

5. Расставьте в правильной последовательности объемы обрабатываемой информации в защищенной информационной системе в порядке возрастания

a) ДзеттаБайты
b) ПетаБайты
c) Гигабайты
d) Терабайты
e) ЭкзаБайты

5. Какой самый высокий класс защиты присваивается системам обнаружения вторжений при проведении аттестации ИСПдн, в которых не обрабатывается гос. тайна, согласно требованиям, утвержденным приказом ФСТЭК России № 638 от 6 декабря 2011 года?

6. **_____** защищаемой информации – это свойство информации, отражающее истинное положение дел

7. Основная функция процессора с точки зрения работы с данными программ?

8. Как называется клавишное устройство управления персональным компьютером, служащее для ввода алфавитно-цифровых (знаковых) данных, а также команд управления?

9. Как называется основное устройство для долговременного хранения больших объемов данных и программ, состоящее из группы соосных дисков, имеющих магнитное покрытие и вращающихся с высокой скоростью?

10. Монитор и сетевой _____ служат в защищенных информационных системах для вывода данных.

Примерные тестовые задания

(проверка сформированности компетенций – ОПК-1)

1. Какой центр занимается вопросами обнаружения, предупреждения и ликвидации последствий компьютерных атак и реагирования на компьютерные инциденты объектов КИИ?

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

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

4. Если различным группам пользователей с различным уровнем доступа требуется доступ к одной и той же информации, что следует предпринять руководству?

5. Расположите сетевые уровни в правильной последовательности в порядке убывания – от верхнего уровня к нижнему модели **OSI** (The Open Systems Interconnection model).

a) Представительский уровень
b) Прикладной уровень
c) Сетевой уровень
d) Транспортный уровень
e) Канальный уровень
f) Сеансовый уровень
g) Физический уровень

6. При защите информации необходимо обеспечивать достаточный уровень безопасности информации, включающей в себя следующие принципы защиты: конфиденциальность, доступность и _____ ?

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

9. Расположите классы защищенности согласно требованиям РД ФСТЭК (Гостехкомиссии) “Классификация автоматизированных систем (АС) по уровню защищенности от несанкционированного доступа (НСД)” в правильной последовательности в порядке убывания

a) 3 А
b) 2 А
c) 3 Б
d) 1 А
e) 2 Б
f) 1 Б

10. Расположите нормативно-правовые документы при работе в защищенных информационных системах по уровню юридической значимости в правильной последовательности в порядке убывания

a) Методические указания Минцифры
b) Постановления правительства
c) Указы президента
d) Конституция РФ
e) Приказы ФСТЭК России

Примерные тестовые задания

(проверка сформированности компетенций – ОПК-2)

1. Сущность комплексного подхода к защите информации – это _____ процесс, проводимый с использованием всех существующих методов и средств?

2.Что такое информационная безопасность?

3. Для работы симметричных криптоалгоритмов требуются защищенный канал передачи данных и _____ключ?

4. Что относится к локальному уровню правового регулирования информационной безопасности?

Утверждение перечня конфиденциальных сведений

a) Постановления федеральных органов власти
b) Указы Президента
c) Федеральные законы

5. Какие виды антивирусных программ принципиально могут обнаруживать только уже известные вредоносные программы?

Дисковые ревизоры

a) Средства обнаружения вторжений
b) Сканеры уязвимостей
c) Сканеры вредоносного программного обеспечения

6.Какой из режимов криптосистемы DES может использоваться для проверки целостности шифра?

a) Перемешивания блоков шифра
b) Преобразование шифра с обратной связью
c) Сцепления блоков шифра

7. Что не относится к аппаратным средствам защиты информации?

a) Криптомаршрутизаторы
b) Модули доверенной загрузки
c) Электронные замки
d) Криптопроцессоры
e) Средства пожарной сигнализации

8. Для чего предназначена программа syskey в ОС Windows?
a) Для логирования нажатий клавиш
b) Для управлению мышью
c) Для считывания информации с датчиков
d) Для шифрования хешей паролей пользователей

9. Что не может использоваться при биометрической аутентификации?

10. Где хранится информация об ограничениях на возможности работы локального пользователя операционной системы Windows?

Промежуточная аттестация (экзамен)

Примерные вопросы к **экзамену**

№	Вопрос
1.	Понятие «информационная система». Концепция безопасности информационной системы. Цели обеспечения информационной безопасности. Санкционированный и несанкционированный доступ.
2.	Угрозы безопасности и каналы реализации угроз. Уровни защиты информации. Стандарты безопасности.
3.	Классы защищённости информационных систем.
4.	Нормативная база Российской Федерации и иностранных государств. Современная доктрина информационной безопасности Российской Федерации.
5.	Трёхуровневая архитектура информационных систем на основе баз данных. Модели данных.
6.	Структура данных. Целостность реляционных данных. Основные этапы проектирования баз данных.
7.	Технологии проектирования на основе нормализации.
8.	Технологии проектирования на основе модели «Сущность-связь».
9.	Основные понятия систем разграничения доступа. Сущность и определение политики безопасности.
10.	Основные типы политик безопасности.
11.	Угрозы целостности информации. Способы противодействия. Понятие и основные свойства транзакций.
12.	Положение о конфиденциальной информации в электронном виде. Контентная категоризация.
13.	Классификация информации по уровню конфиденциальности. Метки документов.
14.	Способы хранение конфиденциальной информации.
15.	Защита документов. Защита каналов утечки конфиденциальной информации. Мониторинг действий пользователей.
16.	Количественный анализ рисков. ALE - annual loss expectancy, ожидаемые годовые потери, т.е. «стоимость» всех инцидентов за год.
17.	Качественный анализ рисков. Метод Дельфи, мозговой штурм, оценка «экспертным методом».
18.	Автоматизированные инструменты для анализа рисков

19.	Оценка ущерба. Классификация внутренних нарушителей.
20.	Особенности проектирования защищенных информационных систем для коммерческой и военной организации.
21.	Тактическое и стратегическое планирование. Работа с кадрами.
22.	Другие градации. Кадровая политика. Определение прав локальных пользователей.
23.	Стандартизация программного обеспечения. Организация процедуры хранения физических носителей информации.
24.	Определение уровней контроля информационных потоков. Режимы архива, сигнализации, активной защиты.
25.	Классификация МЭ. Установление TCP-соединения. Пакетные фильтры, набор правил. Пограничные маршрутизаторы.
26.	Трансляция сетевых адресов (NAT).
27.	Политика МЭ. Реализация его набора правил. Тестирование политики МЭ.
28.	Возможные подходы к эксплуатации МЭ.
29.	Сопровождение МЭ и управление им.
30.	Физическая безопасность окружения МЭ.
31.	Администрирование МЭ.
32.	Стратегия восстановления после сбоев. Возможность создания логов МЭ. Инциденты безопасности.
33.	Понятие системы обнаружения атак. Типы и базовая структура IDS. Совместное расположение Host и Target.
34.	Активные и пассивные ответные действия. Использование SNMP TRAPS.
35.	Системы анализа и оценки уязвимостей. Host-based и Network-based анализ уязвимостей. Способы взаимодействия сканера уязвимостей и IDS.
36.	Сервисы DNS. Инфраструктура DNS. Компоненты DNS и понятие безопасности.
37.	Основные механизмы безопасности для сервисов DNS. Данные DNS и ПО DNS.
38.	Транзакции DNS. Запрос/ответ DNS. Зонная пересылка.
39.	Динамические обновления. Безопасность окружения DNS. Угрозы для ПО и данных DNS.
40.	Причины уязвимости WEB-сервера. Планирование развёртывания WEB-сервера. Безопасное инсталлирование и конфигурирование используемой ОС.
41.	Удаление или запрещение ненужных сервисов и приложений. Управление ресурсами на уровне ОС. Альтернативные платформы для WEB-сервера. Использование Appliances для WEB-сервера. Специально усиленные ОС и WEB-серверы. Тестирование безопасности ОС.
42.	Безопасное инсталлирование и конфигурирование WEB-сервера. Соответствующий список действий.
43.	Разграничение доступа для ПО WEB-сервера. Управление доступом к директории содержимого WEB-сервера. Публикации информации на WEB-сайтах.
44.	Обеспечение безопасности технологий создания активного содержимого.
45.	URLs и cookies. Уязвимости технологий активного содержимого на стороне клиента.
46.	Уязвимости технологий создания содержимого на стороне сервера. Необходимые действия для обеспечения безопасности WEB-содержимого.
47.	Требования к аутентификации и шифрованию. Аутентификация, основанная на IP-адресе. Basic и Digest аутентификации.
48.	SSL/TLS. Возможности и слабые места SSL/TLS. Пример SSL/TLS сессии. Схемы шифрования SSL/TLS.
49.	Ценностно-ориентированные манипулятивные технологии делового общения, используемые в информационных системах для контроля защищаемой информации.
50.	Персональная дистанция в процессе общения. Мишени манипулятивного воздействия при реализации организационных мер защиты информации.

51.	«Малый разговор» в деловой коммуникации. Понятие Адресат манипуляции в деловом общении в рамках управления ИБ.
52.	Техники активной защиты: «Ложного вовлечения», психического воздействия , запутывания, скрытого принуждения.
53.	Техники пассивной зашиты в рамках реализации организационных мер.
54.	Средства невербальной коммуникации. Методы Кинесики, Проксемики и Такетики.
55.	Периферийное оборудование пользователей информационных систем.
56.	Архитектура защищенных информационных систем. Системные шины. Стандарты ISA/PCI/PCI-E/M2.
57.	ГОСТ Р 51583-2014. «Защита информации. Порядок создания автоматизированных систем в защищенном исполнении. Общие положения».
58.	ГОСТ 34.602–2020 «Техническое задание на создание автоматизированной системы».
59.	ГОСТ Р 59793–2021 «Комплекс стандартов на автоматизированные системы. Автоматизированные системы. Стадии создания».

6. Учебно-методическое и информационное обеспечение дисциплины

6.1. Список источников и литературы

Источники

основные

1. *Федеральный закон* «Об информации, информационных технологиях и о защите информации» от 27.07.2006 № 149-ФЗ [Электронный ресурс] : Режим доступа : http://www.consultant.ru/document/cons_doc_LAW_61798/, свободный. – Загл. с экрана.
2. *Федеральный закон* «О персональных данных» от 27.07.2006 № 152-ФЗ (последняя редакция). Электронный ресурс] : Режим доступа : http://www.consultant.ru/document/cons_doc_LAW_61801/, свободный. – Загл. с экрана.
3. *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.
4. *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.
5. *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.

6. *Приказ ФСТЭК России* от 11.02.2013 № 17 «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.
7. *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.
8. *Национальный стандарт РФ ГОСТ Р 70262.1-2022* "Защита информации. Идентификация и аутентификация. Уровни доверия идентификации" (утв. и введен в действие приказом Федерального агентства по техническому регулированию и метрологии от 5 августа 2022 г. N 740-ст) [Электронный ресурс] : Режим доступа : https://docs.cntd.ru/document/1200192541#, свободный. – Загл. с экрана.
9. *Национальный стандарт РФ ГОСТ Р 59453.1-2021* "Защита информации. Формальная модель управления доступом. Часть 1. Общие положения" (утв. и введен в действие приказом Федерального агентства по техническому регулированию и метрологии от 22 апреля 2021 г. N 270-ст) [Электронный ресурс] : Режим доступа : https://docs.cntd.ru/document/1200179191#, свободный. – Загл. с экрана.
10. *Национальный стандарт РФ ГОСТ Р 59453.1-2021* "Защита информации. Формальная модель управления доступом. Часть 2. Общие положения" (утв. и введен в действие приказом Федерального агентства по техническому регулированию и метрологии от 22 апреля 2021 г. N 270-ст) [Электронный ресурс] : Режим доступа : https://docs.cntd.ru/document/1200179192#, свободный. – Загл. с экрана.

Литература

основная

1. Музипов, Х. Н. Программно-технические комплексы автоматизированных систем управления : учебное пособие / Х. Н. Музипов. — Санкт-Петербург : Лань, 2022. — 164 с. — ISBN 978-5-8114-3133-5. — Текст : электронный // Лань : электронно-библиотечная система. — URL: https://e.lanbook.com/book/213098

2. Маршаков, Д. В. Программно-аппаратные средства защиты информации : учебное пособие / Д. В. Маршаков, Д. В. Фатхи. — Ростов-на-Дону : Донской ГТУ, 2021. — 228 с. — ISBN 978-5-7890-1878-1. — Текст : электронный // Лань : электронно-библиотечная система. — URL: https://e.lanbook.com/book/237770

3. Фомин, Д. В. Информационная безопасность и защита информации: специализированные аттестованные программные и программно-аппаратные средства : методические указания / Д. В. Фомин. — Благовещенск : АмГУ, 2017. — 240 с. — Текст : электронный // Лань : электронно-библиотечная система. — URL: https://e.lanbook.com/book/156494

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 : URL: https://bdu.fstec.ru/threat, свободный. – Загл. с экрана.

2. *Методика* определения актуальных угроз безопасности персональных данных при их обработке в информационных системах персональных данных. Утверждена Заместителем директора ФСТЭК России 14 февраля 2008 г. [Электронный ресурс] / ФСТЭК России. – Режим доступа : https://fstec.ru/tekhnicheskaya-zashchita-informatsii/dokumenty/114 -spetsialnye-normativnye-dokumenty/380, свободный. – Загл. с экрана.
3. *Видео уроки* Cisco Packet Tracer. Курс молодого бойца. [Электронный ресурс] : Режим доступа : https://www.youtube.com/playlist?list=PLcDkQ2Au8aVNYsqGsxRQxYyQijILa94T9, 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

1) для лекционных занятий – лекционный класс с видеопроектором и компьютером, на котором должно быть установлено следующее ПО:

№п/п	Наименование ПО	Производитель	Способ распространения (*лицензионное или свободно распространяемое*)
1	Microsoft Office 2010	Microsoft	лицензионное
2	Windows 10 Pro	Microsoft	лицензионное
3	Kaspersky Endpoint Security	Kaspersky	лицензионное

2) для практических занятий – компьютерный класс, оборудованный современными персональными компьютерами для каждого студента. На компьютере должны быть установлено следующее ПО:

№п/п	Наименование ПО	Производитель	Способ распространения (*лицензионное или свободно распространяемое*)
1	Microsoft Office 2010 или выше	Microsoft	лицензионное
2		Microsoft	лицензионное
3	Kaspersky Endpoint Security	Kaspersky	лицензионное
4	Cisco Packet Tracer v.7.2	Cisco Systems	условно свободное (необходима регистрация в сетевой академии Cisco)
5	VMware Workstation 15 Player	VMware, Inc	свободное
6	или VirtualBox 6.0	Oracle	свободное
7	Дистрибутивы Linux (например Ubuntu 14)	Oracle	свободное
8	WEB-сервер Apache 2.0	Apache Software Foundation	свободное
9	Microsoft SQL Server 2008 R2	Microsoft	свободное

Средства вычислительной техники, сетевое оборудование, техническое, программное и программно-аппаратные средства защиты информации и средствами контроля защищенности информации.

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 практических занятий

Темы учебной дисциплины предусматривают проведение практических занятий, которые служат как целям текущего и промежуточного контроля подготовки студентов, так и целям получения практических навыков 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 для практических занятий, выдаваемые преподавателем на каждом занятии.

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

Тематика практических занятий соответствует программе дисциплины.

Практическое занятие 1

Тема – Обеспечение целостности информационных систем на основе баз данных

Задания:

1. Разработать макет базы данных в MS SQLServer.
2. Провести нормализацию отношений (таблиц).
3. Ввести в каждую таблицу не менее пяти строк.
4. Создать формы или представления
5. В полученной базе данных в СУБД Microsoft SQL Server создать таблицы персонала, где должны быть указаны подразделения и сотрудники: кадров, руководства, бухгалтерии, финансового подразделения, менеджеров по работе с клиентами, поставок, заказов, склада и т.д.
6. Присвоить соответствующие роли.
7. Создать правила разграничения доступа на основе ролей.
8. Ответить на теоретические вопросы в конце практической работы.

Указания по выполнению заданий:

1. Изучить теоретический материал по теме.
2. Оформить отчёт по практической работе. Приложением к отчёту служат файлы БД

Материально-техническое обеспечение занятия:

1. Компьютеры по количеству обучающихся с развёрнутой ОС Windows 10 Pro и Microsoft Office 2010.
2. Виртуальная машинас установленной СУБД Microsoft SQL Server

Практическое занятие 2

Тема – Организационные меры защиты информации в организации

Задания:

1. Выбрать организацию из списка предложенных преподавателем.
2. Предложить организационные меры защиты инфрмации.

Указания по выполнению заданий:

1. Изучить теоретический материал по теме.
2. Составить отчёт о практическом занятии.
3. Ответить на теоретические вопросы в конце практического занятия

Материально-техническое обеспечение занятия:

1. Компьютеры по количеству обучающихся с развёрнутой Windows 10 Pro и Microsoft Office 2010, Cisco Packet Tracer

Практическое занятие 3

Тема – Администрирование межсетевых

Задания:

1. Администрирование межсетевого экрана в ОС Linux и Windows
2. Работа с межсетевым экраном Cisco ASA.
3. Администрирование межсетевых экранов в программе Cisco Packet Tracer.

Указания по выполнению заданий:

1. Изучить теоретический материал по теме.
2. На виртуальных машинах установить ОС Linux и Windows (лучше это сделать заранее). Настроить личную учётную запись, выданную преподавателем.
3. Настроить программные межсетевые экраны в ОС. Продемонстрировать их работу.
4. Собрать схему по топологии в Cisco Packet Tracer в индивидуальном адресном пространстве.
5. При работе в чужом адресном пространстве или с чужой учётной записью задание считается невыполненным.
6. Составить отчёт о практическом занятии.
7. Ответить на теоретические вопросы в конце практического занятия

Материально-техническое обеспечение занятия:

1. Компьютеры по количеству обучающихся с развёрнутой Windows 10 Pro и Microsoft Office 2010, Cisco Packet Tracer
2. Развёрнутые виртуальные машины в количестве 2 шт. на каждом ПК с ОС Linux и Windows

Практическое занятие 4

Тема – Безопасное использование службы доменных имён

Задания:

1. Собрать в Cisco Packet Tracer выданную преподавателем схему.
2. Провести настройку DNS-сервера.
3. Присвоить имена компьютерам.
4. Провести имитацию атаки на сервер.

Указания по выполнению заданий:

1. Изучить теоретический материал по теме.
2. Использовать IP-адреса только из своего адресного пространства.
3. При работе в чужом адресном пространстве или с чужой учётной записью задание считается невыполненным.
4. Составить отчёт о практическом занятии.
5. Ответить на теоретические вопросы в конце практического занятия

Материально-техническое обеспечение занятия:

1. Компьютеры по количеству обучающихся с развёрнутой Windows 10 Pro и Microsoft Office 2010, Cisco Packet Tracer

Практическое занятие 5

Тема – Настройка WEB-сервера

Задания:

1. Развернуть а ПК сервер Apache 2.0, MySQL и PHP.
2. Провести настройку WEB-сервера с учётом защиты информации.
3. Создать простой сайт с использованием СУБД MySQL.
4. Атаковать сайт с использованием SQL-инъекций.
5. Добавить код с использованием встроенных функций защиты PHP.
6. Атаковать сайт с использованием SQL-инъекций.

Указания по выполнению заданий:

1. Изучить теоретический материал по теме.
2. Составить отчёт о практическом занятии.
3. Ответить на теоретические вопросы в конце практического занятия

Материально-техническое обеспечение занятия:

2. Компьютеры по количеству обучающихся с развёрнутой Windows 10 Pro и Microsoft Office 2010, Apache 2.0, MySQL и PHP

Практическое занятие 6

Тема – Изучение протокола RADIUS

Задания:

1. Собрать в Cisco Packet Tracer выданную преподавателем схему.
2. Настроить центр авторизации AAA.
3. Провести настройку DNS-сервера.
4. Присвоить имена компьютерам.
5. Провести имитацию атаки на сервер.

Указания по выполнению заданий:

1. Изучить теоретический материал по теме.
2. Собрать схемы по топологии в Cisco Packet Tracer в индивидуальном адресном пространстве.
3. При работе в чужом адресном пространстве задание считается невыполненным.
4. Составить отчёт о практическом занятии.
5. Ответить на теоретические вопросы в конце практического занятия

Материально-техническое обеспечение занятия:

1. Компьютеры по количеству обучающихся с развёрнутой Windows 10 Pro и Microsoft Office 2010, Cisco Packet Tracer

Приложение 1 Аннотация
рабочей программы дисциплины

АННОТАЦИЯ РАБОЧЕЙ ПРОГРАММЫ ДИСЦИПЛИНЫ

Дисциплина «Защищённые информационные системы» реализуется на факультете Информационных систем и безопасности для студентов 1-го курса, обучающихся по программе магистратуры по направлению подготовки 10.04.01 Информационная безопасность (профиль подготовки – Организация и технологии защиты государственной тайны) кафедрой комплексной защиты информации.

Цель дисциплины: профессиональная подготовка магистрантов, необходимая для освоения методов и технологий защиты информационных систем.

Задачи дисциплины: освоение основных понятий и терминологии, технологий и навыков настройки и эксплуатации защищённых информационных систем, изучение нормативных правовых актов в области защищённых информационных систем, архитектуры защищённых информационных систем.

Дисциплина направлена на формирование следующих компетенций:

- УК-4 – Способен применять современные коммуникативные технологии, в том числе на иностранном(ых) языке(ах), для академического и профессионального взаимодействия
- ОПК-1 – Способен обосновывать требования к системе обеспечения информационной безопасности и разрабатывать проект технического задания на ее создание
- ОПК-2 – Способен разрабатывать технический проект системы (подсистемы либо компонента системы) обеспечения информационной безопасности

В результате освоения дисциплины обучающийся должен:

Знать:

- современные коммуникативные технологии на государственном и иностранном языках; закономерности деловой устной и письменной коммуникации;
- основы отечественных и зарубежных стандартов в области обеспечения информационной безопасности;
- методы концептуального проектирования технологий обеспечения информационной безопасности;

Уметь:

- применять на практике коммуникативные технологии, методы и способы делового общения;
- проектировать информационные системы с учётом различных технологий обеспечения информационной безопасности;
- выбирать и обосновывать преимущества методов решения задач для защиты информации компьютерных систем и сетей и систем обеспечения информационной безопасности.

Владеть:

- методикой межличностного делового общения на государственном и иностранном языках, с применением профессиональных языковых форм и средств;
- навыками участия в разработке системы обеспечения информационной безопасности объекта языковых форм и средств;
- навыками выполнения работы по осуществлению при изготовлении, монтаже, наладке, испытаниях и сдаче в эксплуатацию систем и средств обеспечения информационной безопасности.

По дисциплине предусмотрена промежуточная аттестация в форме *экзамена*.

Общая трудоёмкость освоения дисциплины составляет 5 зачётных единиц.

Приложение 2

ЛИСТ ИЗМЕНЕНИЙ

№	Текст актуализации или прилагаемый к РПД документ, содержащий изменения	Дата	№ протокола
1	*Обновлена основная литература*	23.03.2023	***8***

Приложение 1
к листу изменений

Обновление основной литературы (2023 г.)

1. В раздел **6. Учебно-методическое и информационное обеспечение дисциплины** вносятся следующие изменения:
1. Дополнить раздел **Основная литература**

Никифоров, С. Н. Методы защиты информации. Защита от внешних вторжений / С. Н. Никифоров. — 5-е изд., стер. — Санкт-Петербург : Лань, 2023. — 96 с. — ISBN 978-5-507-45868-4. — Текст : электронный // Лань : электронно-библиотечная си-стема. — URL: https://e.lanbook.com/book/288974

Прохорова, О. В. Информационная безопасность и защита информации / О. В. Прохорова. — 5-е изд., стер. — Санкт-Петербург : Лань, 2023. — 124 с. — ISBN 978-5-507-46010-6. — Текст : электронный // Лань : электронно-библиотечная си-стема. — URL: https://e.lanbook.com/book/293009

Составитель:
Кандидат технических наук,
доцент кафедры комплексной защиты информации
А.С. Моляков