МИНИСТЕРСТВО НАУКИ И ВЫСШЕГО ОБРАЗОВАНИЯ РОССИЙСКОЙ ФЕДЕРАЦИИ

ФГБОУ ВО «Уральский государственный экономический университет»

Одобрена
на заседании кафедры

09.12.2025 г.

протокол № 12

И.о. зав. кафедрой Кольева Н.С.

Утверждена
Советом по учебно-методическим вопросам и качеству образования

16 декабря 2025 г.

протокол № 4

Председатель _____ Карх Д.А.
(подпись)

РАБОЧАЯ ПРОГРАММА ДИСЦИПЛИНЫ

Наименование дисциплины	Информационная безопасность и защита информации
Направление подготовки	09.03.03 Прикладная информатика
Профиль	Инжиниринг предприятий и информационных систем
Форма обучения	очная
Год набора	2026

Разработана:
Доцент, к.п.н.
Кольева Н.С.

Ст. преподаватель
Панова М.В.

Екатеринбург
2025 г.

СОДЕРЖАНИЕ

ВВЕДЕНИЕ

Рабочая программа дисциплины является частью основной профессиональнойобразовательной программы высшего образования - программы бакалавриата, разработанной всоответствии с ФГОС ВО

ФГОС ВО	Федеральный государственный образовательный стандарт высшего образования- бакалавриат по направлению подготовки 09.03.03 Прикладная информатика(приказ Минобрнауки России от

1. ЦЕЛЬ ОСВОЕНИЯ ДИСЦИПЛИНЫ

Целью освоения дисциплины «Информационная безопасность и защита информации»является формирование у студентов способности анализировать способы нарушенийинформационной безопасности, изучение методов защиты информационных систем, моделейбезопасности и их применения. Вместе с другими предметами изучение данной дисциплины должноспособствовать расширению профессионального кругозора студентов.

2. МЕСТО ДИСЦИПЛИНЫ В СТРУКТУРЕ ОПОП

Дисциплина относится к обязательной части учебного плана.

3. ОБЪЕМ ДИСЦИПЛИНЫ

Промежуточнаяаттестация	Часов					З.е.
	Всего засеместр	Контактная работа .(поуч.зан.)			Самостоятельная работа в том числеподготовкаконтрольных икурсовых	
		Всего	Лекции	Лабораторные		
Семестр 6						
Зачет	108	64	32	32	44	3

4.ПЛАНИРУЕМЫЕ РЕЗУЛЬТАТЫ ОСВОЕНИЯ ОПОП

В результате освоения ОПОП у выпускника должны быть сформированы компетенции,установленные в соответствии ФГОС ВО.

Шифр и наименованиекомпетенции	Индикаторы достижения компетенций
ОПК-3 Способен решатьстандартные задачипрофессиональнойдеятельности на основеинформационной ибиблиографическойкультуры с применениеминформационно-коммуникационныхтехнологий и с учетомосновных требованийинформационнойбезопасности;	ИД-1.ОПК-3 Знать: принципы, методы и средства решениястандартных задач профессиональной деятельности на основеинформационной и библиографической культуры с применениеминформационно-коммуникационных технологий и с учетом основныхтребований информационной безопасности.

ОПК-3 Способен решатьстандартные задачипрофессиональнойдеятельности на основеинформационной ибиблиографическойкультуры с применениеминформационно-коммуникационныхтехнологий и с учетомосновных требованийинформационнойбезопасности;	ИД-2.ОПК-3 Уметь: решать стандартные задачи профессиональнойдеятельности на основе информационной и библиографическойкультуры с применением информационно-коммуникационныхтехнологий и с учетом основных требований информационнойбезопасности.
	ИД-3.ОПК-3 Иметь практический опыт: подготовки обзоров,аннотаций, составления рефератов, научных докладов, публикаций, ибиблиографии по научно-исследовательской работе с учетомтребований информационной безопасности

5. ТЕМАТИЧЕСКИЙ ПЛАН

Тема	Часов						
	Наименование темы	Всего часов	Контактная работа .(по уч.зан.)			Самост.работа	Контрольсамостоятельной работы
			Лекции	Лабораторные	Практическиезанятия		
Семестр 6		10					
Тема 1.	Международные стандартыинформационного обмена. Понятиеугрозы. Информационная безопасностьв условиях функционирования в Россииглобальных сетей. Виды противниковили	34	4	20		10	
Тема 2.	Три вида возможных нарушенийинформационной системы. Защита.Основные нормативные руководящиедокументы,	10	4			6	
Тема 3.	Нормативно-справочные документы.Назначение и задачи в сфере обеспеченияинформационной	6	4			2	

Тема 4.	Основные положения теорииинформационной безопасностиинформационных систем. Моделибезопасности и их применение.Таксономия нарушений информационнойбезопасности вычислительной системыи причины, обуславливающие ихсуществование.	28	4	12		12	
Тема 5.	Анализ способов нарушенийинформационной безопасности.Использование защищенныхкомпьютерных систем.	14	4			10	
Тема 6.	Методы криптографии	10	8			2	
Тема 7.	Основные технологии построениязащищенных	6	4			2	

6. ФОРМЫ ТЕКУЩЕГО КОНТРОЛЯ И ПРОМЕЖУТОЧНОЙ АТТЕСТАЦИИ ШКАЛЫ ОЦЕНИВАНИЯ

Раздел/Тема	Вид оценочногосредств	Описание оценочного средства	Критериоценивания
Текущий контроль (Приложение 4)			
Темы 1-3	Контрольная работа	Контрольная работа содержит 1 задание	10 баллов
Тема 4-6	Контрольнаяработа (приложение 4)	Контрольная работа содержит 1задание	10 баллов
Тема 7	Контрольнаяработа (приложение 4)	Контрольная работа содержит 1 задание	10 баллов
Промежуточная аттестация(Приложение 5)			
6 семестр (За)	Билет для зачета (приложение 5)	Билет включает в себя один теоретическийвопрос и одно практическое	100 баллов

ОПИСАНИЕ ШКАЛ ОЦЕНИВАНИЯ

Показатель оценки освоения ОПОП формируется на основе объединения текущего контроляи промежуточной аттестации обучающегося.

Показатель рейтинга по каждой дисциплине выражается в процентах, который показываетуровень подготовки студента.

Текущий контроль.Используется 100-балльная система оценивания. Оценка работы студента втечении семестра осуществляется преподавателем в соответствии с разработанной им системойоценки учебных достижений в процессе обучения по данной дисциплине.

В рабочих программах дисциплин и практик закреплены виды текущего контроля,планируемые результаты контрольных мероприятий и критерии оценки учебный достижений.

В течение семестра преподавателем проводится не менее 3-х контрольных мероприятий, поооценке деятельности студента. Если посещения занятий по дисциплине включены в рейтинг, тоданный показатель составляет не более 20% от максимального количества баллов по дисциплине.

Промежуточная аттестация. Используется 5-балльная система оценивания. Оценка работыстудента по окончанию дисциплины (части дисциплины) осуществляется преподавателем всоответствии с разработанной им системой оценки достижений студента в процессе обучения поданной дисциплине. Промежуточная аттестация также проводится по окончанию формированиякомпетенций.

Порядок перевода рейтинга, предусмотренных системой оценивания, по дисциплине, впятибалльную систему.

Высокий уровень – 100% - 70% - отлично, хорошо.

Средний уровень – 69% - 50% - удовлетворительно.

Показатель оценки	По 5-балльной системе	Характеристика показателя
100% - 85%	отлично	обладают теоретическими знаниями в полном объеме,понимают, самостоятельно умеют применять,исследовать, идентифицировать, анализировать,систематизировать, распределять по категориям,рассчитать показатели, классифицировать,разрабатывать модели, алгоритмизировать, управлять,организовать, планировать процессы исследования,осуществлять оценку результатов на высоком уровне
84% - 70%	хорошо	обладают теоретическими знаниями в полном объеме,понимают, самостоятельно умеют применять,исследовать, идентифицировать, анализировать,систематизировать, распределять по категориям,рассчитать показатели, классифицировать,разрабатывать модели, алгоритмизировать, управлять,организовать, планировать процессы исследования,осуществлять оценку результатов. Могут быть допущены недочеты, исправленныестудентом самостоятельно в процессе работы (ответаи т.д.)
69% - 50%	удовлетворительно	обладают общими теоретическими знаниями, умеютприменять, исследовать, идентифицировать,анализировать, систематизировать, распределять покатегориям, рассчитать показатели,классифицировать, разрабатывать модели,алгоритмизировать, управлять, организовать,планировать процессы исследования, осуществлятьоценку результатов на среднем уровне. Допускаются ошибки, которые студент затрудняетсяисправить самостоятельно.
49 % и менее	неудовлетворительно	обладают не полным объемом общих теоретическимизнаниями, не умеют самостоятельно применять,исследовать, идентифицировать, анализировать,систематизировать, распределять по категориям,рассчитать показатели, классифицировать,разрабатывать модели, алгоритмизировать, управлять,организовать, планировать процессы исследования,осуществлять оценку результатов. Не сформированы умения и навыки для
100% - 50%	зачтено	характеристика показателя соответствует «отлично»,«хорошо», «удовлетворительно»
49 % и менее	не зачтено	характеристика показателя соответствует«неудовлетворительно»

7. СОДЕРЖАНИЕ ДИСЦИПЛИНЫ

7.1. Содержание лекций

Тема 1. Международные стандарты информационного обмена. Понятие угрозы. Информационнаябезопасность в условиях функционирования в России глобальных сетей. Виды противников или«нарушителей». Понятия о видах вирусов.

1.1 Основные концептуальные положения системы защиты информации. Понятие информации.Структура защиты информации. Условия и требования, которым должна удовлетворять системазащиты информации. Виды собственного обеспечения системы защиты информации.
1.2 Концептуальная модель информационной безопасности. Объекты угроз. Угрозыконфиденциальной информации. Конфиденциальность, полнота (целостность), достоверность идоступность информации. Ущерб от угрозы информационной безопасности.
1.3 Классификация угроз по величине принесенного ущерба, по вероятности возникновения, попричинам появления, по характеру нанесенного ущерба.
Действия, приводящие к неправомерному овладению информацией. Разглашение. Утечка.Несанкционированный доступ.

Тема 2. Три вида возможных нарушений информационной системы. Защита. Основные нормативныеруководящие документы, касающиеся государственной тайны.
2.1 Правовое регулирование защиты информации. Выполнение участниками информационныхправоотношений и контроль выполнения полномочными субъектами, в т.ч. правоохранительными,норм права, содержащих организационно-технические требования, дозволения и запреты в целяхобеспечения целостности, доступности и конфиденциальности информации.
Интересы личности в информационной сфере. Интересы общества в информационной сфере.Интересы государства в информационной сфере.
2.2 Структура норм права Российской Федерации. Законодательства Российской Федерации вобласти защиты информации. Направления правого регулирования защиты информации.Конституционные гарантии интересов личности в информационной сфере.
Собственник, владелец и пользователь информационных ресурсов. Информация, не относящаяся ктайне, но распространение, которой ограничено (запрещено). Служебная или коммерческая тайна.
Руководящие документы Гостехкомиссии.
Административные правонарушения в сфере защиты информации. Составы преступлений,предусмотренные за нарушение режима защиты информации.
Электронная цифровая подпись. Закон об электронной цифровой подписи.

Тема 3. Нормативно-справочные документы. Назначение и задачи в сфере обеспеченияинформационной безопасности на уровне государства.
3.1 Проблемы целостности и конфиденциальности информации на магнитных носителях.
Используемые методы защиты от непосредственного доступа к магнитным носителям.
Интеллектуальные возможности контроллера жесткого магнитного диска. Программное обеспечениедля доступа и управления этими возможностями.
3.2 Физические принципы удаления и восстановления информации на магнитных носителях.Способы уничтожения информации на жестких магнитных дисках.
Обычные способы удаления файлов в файловых системах FAT, NTFS, S5/UFS. Возможностипрограмм «шредеров». Программные и аппаратные средства уничтожения информации на HDD.Гарантированное уничтожение с разрушением магнитного носителя.
Способы восстановления информации на гибких магнитных дисках.

Тема 4. Основные положения теории информационной безопасности информационных систем.Модели безопасности и их применение. Таксономия нарушений информационной безопасностивычислительной системы и причины, обуславливающие их существование.
4.1 Понятие и классификация криптографических методов и средств защиты информации.Шифрование и кодирование. Ключ. Криптостойкость шифра. Характеристика некоторых методовшифрования.
4.2 Структура и классификация криптографических систем. Основные режимы работысимметричных алгоритмов и стандартов шифрования данных. Симметричные и асимметричные (соткрытым ключом) криптосистемы. Алгоритмы их работы.
4.3 Аутентификация электронных документов и сообщений. Системы электронно-цифровойподписи.
4.4 Американские алгоритмы шифрования данных DES, AES, RSA.
Алгоритм шифрования данных по ГОСТ 28147-89.

Тема 5. Анализ способов нарушений информационной безопасности. Использование защищенныхкомпьютерных систем.
5.1 Вредоносные программы. Условия вредоносности. Команды в оболочках Windows, позволяющиекопировать, модифицировать и удалять компьютерную информацию на уровне файлов и каталогов.
Деструктивные возможности стандартных команд. Вызов "опасных" функций в командной строке.Возможности программы RUNDLL32.EXE.
5.2 Разновидности программ. Разновидности вредоносных программ. Клавиатурные перехватчики.«Логические бомбы». Сетевые «черви». «Жадные» программы. Программы «глюки». «Мифические»вирусы.
Происхождение вирусов. Отличительные свойства компьютерных вирусов. Характеристика«традиционных» вирусов. Сущность вирусного заражения.
5.3 Макровирусы. Причины распространения макровирусов. Механизмы вирусного зараженияшаблонов и документов.
Программные и аппаратные закладки. Отличительные свойства программных и аппаратныхзакладок. Функции, реализуемые программными и аппаратными закладками.
Жизненный цикл «вредоносной» программы. Способы запуска вредоносных программ. Социальнаяинженерия.
5.4 Характерные особенности программ удаленного администрирования.
Внедрение и запуск кода с помощью элементов ActiveX. Использование серверов автоматизации вHTML-файлах.
Антивирусное программное обеспечение. Антивирусная профилактика.

Тема 6. Методы криптографии

6.1 Зачем нужны политика безопасности и процедуры безопасности? Выработка официальнойполитики предприятия в области информационной безопасности. Оценка рисков.

Выработка процедур для предупреждения нарушений безопасности. Процедуры выявлениянеавторизованной деятельности.

Типы процедур безопасности. Проверка системной безопасности. Процедуры управления счетами.Процедуры управления паролями. Процедуры конфигурационного управления.

6.2 Реакция на нарушения безопасности. Регистрационная документация.

Примерный перечень регламентирующих документов. Документы, которые носят общий характер,но несут максимальную правовую нагрузку, позволяющие, в случае необходимости, даватьадминистративно-правовую оценку, возбуждать иски.

6.3 Документы, которые разделяют и закрепляют основные функции и обязанности. Документы,которые являются инструкциями для администраторов и пользователей КС и детализируютдействия, права и обязанности пользователей.

6.4 Компьютерная система как источник побочных электромагнитных излучений. Несепарабельноеэлектромагнитное поле. Энергетика и диапазон побочных излучений.

Технические каналы утечки компьютерной информации. Визуально-оптический перехват. Перехватпобочных электромагнитных излучений. Перехват акустических полей.

6.5 Классификация элементов ПЭВМ по степени угроз.

Клавиатура как источник утечки информации. Виды аппаратных закладок в клавиатуре.

Принтеры как источники утечки компьютерной информации по техническим каналам. Четыреканала утечки информации характерные для принтеров.

6.6 Монитор как источник утечки. Плата видеоадаптера как источник побочных электромагнитныхизлучений. Возможная схема перехвата побочных электромагнитных излучений монитора.Аппаратные закладки в видеоканале.

6.7 Способы защиты от перехвата информации с экранов мониторов.

6.8 Требования к программно-аппаратным средствам защиты информации. Меры защитыинформации. Принципы защиты информации.

Характеристики средств защиты информации, создаваемые аппаратно-программными средствами.Функции СЗИ. Схема защиты информации.

6.9 Реализация политики разграничения доступа (Dallas Lock).

Блокирование доступа злоумышленника к закрытым, виртуальным дискам, содержащимконфиденциальные данные и программы их обработки. Способы аутентификации личности.

Организация виртуального диска. Структура файла-образа виртуального диска.

6.10 Резидентные программы-шпионы, которые могут отслеживать процессы, происходящие сданными на компьютере. Чтение остаточной информации в памяти после выполнениясанкционированных запросов.

Сетевые средства защиты информации (ViPNet). Серверная часть программного обеспечения.Клиентская часть программного обеспечения.

Тема 7. Основные технологии построения защищенных информационных систем
7.1 Межсетевой экран (МЭ), Firewall, брандмауэр. Основные компоненты МЭ.
Фильтрующий маршрутизатор. Характеристики фильтрующего маршрутизатора.
Схема инкапсуляции данных в стеке протоколов TCP/IP. Заголовок IP. Заголовок TCP. ЗаголовокUDP. Сообщение ICMP. Пример таблицы фильтрации. Правила внутреннего и внешнего соединенияузлов.
Шлюз сетевого уровня. Дополнительные возможности (NAT, Port Mapping).
Шлюз прикладного уровня. Реализация шлюза прикладного уровня. Функции шлюза прикладногоуровня. "Укрепленный" компьютер. Использование COM-порта.
7.2 Политика межсетевого взаимодействия. Политика сетевой безопасности.
Основные схемы сетевой защиты на базе МЭ.
Двупортовый шлюз. Экранированный шлюз. Экранированная подсеть.
Использование нескольких бастионов. Объединение внутреннего и внешнего маршрутизаторов.Объединение внешнего маршрутизатора с бастионом.
Объединение внутреннего маршрутизатора с бастионом. Использование нескольких внутреннихмаршрутизаторов.
Использование нескольких внутренних подсетей. Использование нескольких внутренних подсетей смагистралью. Использование нескольких внешних маршрутизаторов. Использование нескольких периметровых подсетей.

7.2 Содержание практических занятий и лабораторных работ

Тема 4. Основные положения теории информационной безопасности информационных систем.Модели безопасности и их применение. Таксономия нарушений информационной безопасностивычислительной системы и причины, обуславливающие их существование.

1. основные меры противодействия угрозам безопасности, принципы построения систем защиты,основные механизмы защиты;
2. модели разграничения доступа;
3. криптографические методы защиты, виды средств криптозащиты данных, их достоинства инедостатки, место и роль средств криптозащиты.
4. противодействие угрозам безопасности корпоративной сети со стороны Интернет.
5. правовое регулирование защиты информации в Российской Федерации.

7.3. Содержание самостоятельной работы

Тема 1. Международные стандарты информационного обмена. Понятие угрозы. Информационнаябезопасность в условиях функционирования в России глобальных сетей. Виды противников или«нарушителей». Понятия о видах вирусов. Изучение теоретического материала, основной и дополнительной литературы. Разбор лабораторныхработ. Выполнение практических работ.
Тема 2. Три вида возможных нарушений информационной системы. Защита. Основные нормативныеруководящие документы, касающиеся государственной тайны. Изучение теоретического материала, основной и дополнительной литературы. Разбор лабораторныхработ. Выполнение практических работ.
Тема 3. Нормативно-справочные документы. Назначение и задачи в сфере обеспеченияинформационной безопасности на уровне государства. Изучение теоретического материала, основной и дополнительной литературы. Разбор лабораторныхработ. Выполнение практических работ.
Тема 4. Основные положения теории информационной безопасности информационных систем.Модели безопасности и их применение. Таксономия нарушений информационной безопасностивычислительной системы и причины, обуславливающие их существование. Изучение теоретического материала, основной и дополнительной литературы. Разбор лабораторныхработ. Выполнение практических работ.
Тема 5. Анализ способов нарушений информационной безопасности. Использование защищенныхкомпьютерных систем. Изучение теоретического материала, основной и дополнительной литературы. Разбор лабораторныхработ. Выполнение практических работ.
Тема 6. Методы криптографии Изучение теоретического материала, основной и дополнительной литературы. Разбор лабораторныхработ. Выполнение практических работ.
Тема 7. Основные технологии построения защищенных информационных систем Изучение теоретического материала, основной и дополнительной литературы. Разбор лабораторныхработ. Выполнение практических работ.

7.3.1. Примерные вопросы для самостоятельной подготовки к зачету/экзамену
Приложение 1.

7.3.2. Практические задания по дисциплине для самостоятельной подготовки кзачету/экзамену
Приложение 2.

7.3.3. Перечень курсовых работ
Не предусмотрено.

7.4. Электронное портфолио обучающегося
Материалы не размещаются.

7.5. Методические рекомендации по выполнению контрольной работы
Не предусмотрено.

7.6 Методические рекомендации по выполнению курсовой работы
Не предусмотрено.

8. ОСОБЕННОСТИ ОРГАНИЗАЦИИ ОБРАЗОВАТЕЛЬНОГО ПРОЦЕССА ПО ДИСЦИПЛИНЕ ДЛЯ ЛИЦ С ОГРАНИЧЕННЫМИ ВОЗМОЖНОСТЯМИ ЗДОРОВЬЯ

По заявлению студента

В целях доступности освоения программы для лиц с ограниченными возможностями здоровья при необходимости кафедра обеспечивает следующие условия:

- особый порядок освоения дисциплины, с учетом состояния их здоровья;
- электронные образовательные ресурсы по дисциплине в формах, адаптированных к ограничениям их здоровья;
- изучение дисциплины по индивидуальному учебному плану (вне зависимости от формы обучения);
- электронное обучение и дистанционные образовательные технологии, которые предусматривают возможности приема-передачи информации в доступных для них формах.
- доступ (удаленный доступ), к современным профессиональным базам данных и информационным справочным системам, состав которых определен РПД.

9. ПЕРЕЧЕНЬ ОСНОВНОЙ И ДОПОЛНИТЕЛЬНОЙ УЧЕБНОЙ ЛИТЕРАТУРЫ, НЕОБХОДИМОЙ ДЛЯ ОСВОЕНИЯ ДИСЦИПЛИНЫ

Сайт библиотеки УрГЭУ
http://lib.usue.ru/

Основная литература:

2. Крамаров С.О., Тищенко Е.Н., Соколов С.В., Шевчук П.С., Митясова О.Ю.Криптографическая защита информации [Электронный ресурс]:Учебное пособие : Учебноепособие. - Москва: Издательский Центр РИО, 2025. - 321 – Режим доступа:https://znanium.com/catalog/product/2169480

3. Запечников С. В., Казарин О. В., Тарасов А. А. Криптографические методы защитыинформации [Электронный ресурс]:учебник для вузов. - Москва: Юрайт, 2024. - 309 – Режимдоступа: https://urait.ru/bcode/536453

4. Фомичёв В. М., Мельников Д. А. Криптографические методы защиты информации в 2 ч.Часть 1. Математические аспекты [Электронный ресурс]:учебник для вузов. - Москва: Юрайт, 2024.- 209 – Режим доступа: https://urait.ru/bcode/536733

5. Шейдаков Н.Е., Тищенко Е.Н., Серпенинов О.В. Физические основы защиты информации[Электронный ресурс]:Учебное пособие. - Москва: Издательский Центр РИО, 2026. - 204 – Режимдоступа: https://znanium.com/catalog/product/2084198

6. Гришина Н. В. Основы информационной безопасности предприятия [Электронныйресурс]:Учебное пособие. - Москва: ООО "Научно-издательский центр ИНФРА-М", 2024. - 216 –Режим доступа: https://znanium.com/catalog/product/2131865

7. Ищейнов В. Я., Мецатунян М. В. Организационное и техническое обеспечениеинформационной безопасности. Защита конфиденциальной информации [Электронныйресурс]:Учебное пособие. - Москва: ООО "Научно-издательский центр ИНФРА-М", 2024. - 256 –Режим доступа: https://znanium.com/catalog/product/2139841

8. Казарин О. В., Забабурин А. С. Программно-аппаратные средства защиты информации.Защита программного обеспечения [Электронный ресурс]:учебник и практикум для вузов. - Москва:Юрайт, 2024. - 312 – Режим доступа: https://urait.ru/bcode/538066

Дополнительная литература:

2. Баранова Е.К., Бабаш А.В. Информационная безопасность. История специальных методовкриптографической деятельности [Электронный ресурс]:учебное пособие. - Москва: ИздательскийЦентр РИО, 2022. - 236 – Режим доступа: https://znanium.ru/catalog/product/1843171

3. Шаньгин В.Ф. Комплексная защита информации в корпоративных системах [Электронныйресурс]:Учебное пособие. - Москва: Издательский Дом "ФОРУМ", 2022. - 592 – Режим доступа:https://znanium.com/catalog/product/1843022

4. Васильков А.В., Васильков И. А. Безопасность и управление доступом в информационныхсистемах [Электронный ресурс]:Учебное пособие. - Москва: Издательство "ФОРУМ", 2020. - 368 –Режим доступа: https://znanium.com/catalog/product/1082470

5. Глинская Е.В., Чичварин Н.В. Информационная безопасность конструкций ЭВМ и систем[Электронный ресурс]:Учебное пособие. - Москва: ООО "Научно-издательский центр ИНФРА-М",2021. - 118 с. – Режим доступа: https://znanium.com/catalog/product/1178152

10. ПЕРЕЧЕНЬ ИНФОРМАЦИОННЫХ ТЕХНОЛОГИЙ, ВКЛЮЧАЯ ПЕРЕЧЕНЬ ЛИЦЕНЗИОННОГО ПРОГРАММНОГО ОБЕСПЕЧЕНИЯ И ИНФОРМАЦИОННЫХ СПРАВОЧНЫХ СИСТЕМ, ОНЛАЙН КУРСОВ, ИСПОЛЬЗУЕМЫХ ПРИ ОСУЩЕСТВЛЕНИИ ОБРАЗОВАТЕЛЬНОГО ПРОЦЕССА ПО ДИСЦИПЛИНЕ

Перечень лицензионного программного обеспечения:

Microsoft Windows 10 .Договор № 52/223-ПО/2020 от 13.04.2020, Акт № Tr000523459 от 14.10.2020. Срок действия лицензии -Без ограничения срока.

Microsoft Office 2016.Договор № 52/223-ПО/2020 от 13.04.2020, Акт № Tr000523459 от 14.10.2020 Срок действия лицензии -Без ограничения срока.

Перечень информационных справочных систем, ресурсов информационно-телекоммуникационной сети «Интернет»:

Справочно-правовая система Гарант. Договор № 58419 от 22 декабря 2015. Срок действия лицензии -без ограничения срока

Справочно-правовая система Консультант +. Договор № 143/223-У/2025 от 02.12.2025 Срок действия лицензии до 31.12.2026

Защита информации

https://openedu.ru/course/hse/DATPRO/

11. ОПИСАНИЕ МАТЕРИАЛЬНО-ТЕХНИЧЕСКОЙ БАЗЫ, НЕОБХОДИМОЙ ДЛЯ ОСУЩЕСТВЛЕНИЯ ОБРАЗОВАТЕЛЬНОГО ПРОЦЕССА ПО ДИСЦИПЛИНЕ

Реализация учебной дисциплины осуществляется с использованием материально-технической базы УрГЭУ, обеспечивающей проведение всех видов учебных занятий и научно-исследовательской и самостоятельной работы обучающихся:

Специальные помещения представляют собой учебные аудитории для проведения всех видов занятий, групповых и индивидуальных консультаций, текущего контроля и промежуточной аттестации.

Помещения для самостоятельной работы обучающихся оснащены компьютерной техникой с возможностью подключения к сети "Интернет" и обеспечением доступа в электронную информационно-образовательную среду УрГЭУ.

Все помещения укомплектованы специализированной мебелью и оснащены мультимедийным оборудованием спецоборудованием (информационно-телекоммуникационным, иным компьютерным), доступом к информационно-поисковым, справочно-правовым системам, электронным библиотечным системам, базам данных действующего законодательства, иным информационным ресурсам служащими для представления учебной информации большой аудитории.

Для проведения занятий лекционного типа презентации и другие учебно-наглядные пособия, обеспечивающие тематические иллюстрации.

Приложение 1
к рабочей программе

7.3.1. Примерные вопросы для самостоятельной подготовки к зачету

К зачету

1. Понятие информационной безопасности.
2. Основные составляющие информационной безопасности.
3. Важность проблемы информационной безопасности.
4. Примеры статистики нарушений информационной безопасности.
5. Основные понятия объектно-ориентированного подхода.
6. Уровни мер в области информационной безопасности.
7. Наиболее распространенные угрозы.
8. Российское законодательство в области информационной безопасности.
9. Зарубежное законодательство в области информационной безопасности.
10. Характеристика стандартов и спецификаций в области информационной безопасности.
11. Обзор сильных и слабых сторон стандартов ИБ.
12. Политика безопасности и программа безопасности. Структура соответствующих документов. Меры по их разработке и сопровождению.
13. Меры безопасности, связанные с этапами жизненного цикла информационных систем.
14. Управление рисками. Методика сопоставления возможных потерь от нарушений ИБ и стоимостью защитных средств.
15. Основные классы мер процедурного уровня информационной безопасности.
16. Принципы обеспечения надежной защиты.
17. Понятие сервиса безопасности. Вопросы архитектурной безопасности. Классификация сервисов.
18. Идентификация и аутентификация, управление доступом.
19. Протоколирование и аудит. Криптографические методы защиты.
20. Сервисы безопасности – экранирование и анализ защищенности.

Приложение 2
к рабочей программе

7.3.2. Практические задания по дисциплине для самостоятельной подготовки к зачету

Примерные вопросы закрытого типа

1. Что означает аббревиатура VPN?
    1. Virtual Personal Network
    2. Virtual Private Network
    3. Very Private Network
    4. Virtual Protection Network
2. Какой метод защиты информации предполагает использование биометрических данных?
    1. Шифрование
    2. Биометрическая аутентификация
    3. Фишинг
    4. DDoS-атака
3. Что такое DDoS-атака?
    1. Атака на удаленный сервер
    2. Атака на базу данных
    3. Атака на сеть
    4. Атака на веб-сайт
4. Какой вид угрозы информационной безопасности связан с незаконным доступом к данным?
    1. Вирус
    2. Фишинг
    3. Хакерство
    4. Спам
5. Что такое межсетевой экран (firewall)?
    1. Программа-шпион
    2. Программа-антивирус
    3. Программа-блокировщик рекламы
    4. Программа-брандмауэр

Примерные вопросы открытого типа

1. Как вы оцениваете важность обучения сотрудников по вопросам информационной безопасности для организации?
2. Какие меры безопасности вы считаете наиболее эффективными для защиты конфиденциальной информации в компании?
3. Какие риски для информационной безопасности вы видите в повседневной работе с компьютером и интернетом?
4. Как вы думаете, какие технологии будут наиболее востребованы для обеспечения информационной безопасности в будущем?
5. Какие шаги вы считаете необходимыми для обеспечения безопасности данных при работе с облачными сервисами?

Примерные практические задания к зачету

1. Зашифровать слово КРИПТОГРАФИЯ шифром Тритемиуса с ключом СКИТАЛА.
2. Зашифровать слово КРИПТОАНАЛИЗ шифром Виженера с ключом ЦЕЗАРЬ.
3. Зашифровать слово КРИПТОЛОГИЯ шифром гаммирования с гаммой, равной числу e.
4. Зашифровать слово ПОДСТАНОВКА шифром гаммирования с гаммой, равной числу π.

5. Зашифровать слово ПЕРЕСТАНОВКА шифром гаммирования с гаммой, равной числу e.
6. Зашифровать фразу «Шифр Цезаря относится к детским шифрам» шифром перестановок с перестановочной таблицей размером 6×6 и ключевым словом ЦЕЗАРЬ.
7. Зашифровать фразу «Скитала является механическим шифровальным устройством» шифром перестановок с перестановочной таблицей размером 8×7 и ключевым словом ВИЖЕНЕР.
8. Зашифровать слово КРИПТОГРАФИЯ шифром Тритемиуса с ключом ПОЛИБИЙ.
9. Зашифровать слово КРИПТОАНАЛИЗ шифром Виженера с ключом ШЕННОН.
10. Зашифровать слово КАЗИСКИЙ шифром гаммирования с гаммой, равной числу e.
11. Зашифровать слово КОДИРОВАНИЕ шифром гаммирования с гаммой, равной числу π.
12. Зашифровать слово ШИФРОБЛОКНОТ шифром гаммирования с гаммой, равной числу e.
13. Зашифровать фразу «Шифр Цезаря относится к шифрам замены» шифром перестановок с перестановочной таблицей размером 6×6 и ключевым словом ПАРОЛЬ.
14. Зашифровать фразу «Кодирование является частью криптографии» шифром перестановок с перестановочной таблицей размером 6×7 и ключевым словом ВИЖЕНЕР.
15. Зашифровать фразу «Стеганография не является частью криптографии» шифром перестановок с перестановочной таблицей размером 8×6 и ключевым словом ВЕРНАМ.
16. Зашифровать слово КРИПТОСТОЙКОСТЬ шифром Полибия.