Частное учреждение высшего образования
«Институт государственного администрирования»

.

Кафедра математики и информационных технологий

УТВЕРЖДАЮ
Проректор по учебной работе
_____ П.Н. Рузанов
«29» мая 2025 г.

РАБОЧАЯ ПРОГРАММА УЧЕБНОЙ ДИСЦИПЛИНЫ

Информационная безопасность

Направление подготовки
09.03.01 Информатика и вычислительная техника

Направленность
«Искусственный интеллект и машинное обучение»

ПРОГРАММА БАКАЛАВРИАТА

Квалификация
Бакалавр

Форма обучения

Очная

Москва 2025

Рабочая программа учебной дисциплины ***Информационная безопасность*** разработана на основании федерального государственного образовательного стандарта высшего образования – бакалавриата по направлению подготовки 09.03.01 Информатика и вычислительная техника (бакалавриат), утвержденного приказом Министерства образования и науки Российской Федерации от 19.09.2017 № 929, учебного плана по основной профессиональной образовательной программе высшего образования – программе бакалавриата по направлению подготовки 09.03.01 Информатика и вычислительная техника (бакалавриат), с учетом следующих профессиональных стандартов, сопряженных с профессиональной деятельностью выпускника:

− 06.001 «Программист»;

− 06.004 «Специалист по тестированию в области ИТ»

− 06.011 «Администратор баз данных»;

− 06.015 «Специалист по информационным системам».

− 06.016 «Руководитель проектов в области информационных технологий»

− 06.019 «Технический писатель (специалист по технической документации в области ИТ)

Рабочая программа учебной дисциплины разработана рабочей группой в составе:

Рабочая программа дисциплины (модуля) обсуждена и утверждена на заседании кафедры математики и информационных технологий.

Протокол №

Заведующий кафедрой _____

(подпись)

СОДЕРЖАНИЕ

РАЗДЕЛ 1. ПАСПОРТ РАБОЧЕЙ ПРОГРАММЫ УЧЕБНОЙ ДИСЦИПЛИНЫ

1.1 Цель и задачи учебной дисциплины

Цель учебной дисциплины «Информационная безопасность» является формирование у студентов знаний и представлений о смысле, целях, задачах и методах защиты информации в информационных системах. Приобретенные навыки позволят студентам правильно строить систему информационной безопасности организации и предприятия.

Задачей дисциплины «Информационная безопасность» является изучение организационных, инженерно-технических, криптографических и программно-аппаратных методов защиты информации

Основные задачи дисциплины предусматривают предоставление знаний по следующим вопросам:

- сущность и задачи обеспечения информационной безопасности;
- принципы организации и этапы разработки системы обеспечения информационной безопасности;
- анализ рисков и оценка угроз информационной безопасности;
- определение компонентов системы информационной безопасности предприятия;
- оценка эффективности средств обеспечения информационной безопасности;
- обеспечение криптографической защиты информации;
- защита информации от вредоносных программ.

1.2. Место учебной дисциплины в структуре основной профессиональной образовательной программы

Учебная дисциплина «*Информационная безопасность*» реализуется в обязательной части основной профессиональной образовательной программы высшего образования – программы бакалавриата по направлению подготовки 09.03.01 «Информатика и вычислительная техника» очной, заочной формы обучения**.**

Изучение учебной дисциплины *«Информационная безопасность»* базируется на знаниях и умениях, полученных обучающимися ранее в ходе освоения программного материала ряда учебных дисциплин: *«Программирование», «Физика».*

Перечень последующих учебных дисциплин, для которых необходимы знания, умения и навыки, формируемые данной учебной дисциплиной: *Проектирование и администрирование информационных систем.*

1.3 Планируемые результаты обучения по учебной дисциплине в рамках планируемых результатов освоения основной образовательной программы соотнесенные с установленными индикаторами достижения компетенций

Процесс освоения учебной дисциплины направлен на формирование у обучающихся следующих компетенций: ОПК-3; ПК-7; ПК-11 в соответствии с основной профессиональной образовательной программой высшего образования – программа бакалавриата по направлению подготовки 09.03.01 «Информатика и вычислительная техника» очной, заочной формы обучения**.**

В результате освоения учебной дисциплины обучающийся должен демонстрировать следующие результаты:

ОПК-3; ПК-7; ПК-11

Категория компетенций	**Код компетенции**	**Формулировка компетенции**	**Код и наименование индикатора достижения компетенции**	**Код и наименование индикатора достижения компетенции**
	ОПК-3	Способен решать стандартные задачи профессиональной деятельности на основе информационной и библиографической культуры с применением информационно-коммуникационных технологий и с учетом основных требований информационной безопасности;	ОПК-3.**ИД-1.** Сформирован понятийный аппарат и теоретическая основа для выполнения практических действий в рамках компетенции	ОПК-3.1 Знать: принципы, методы и средства решения стандартных задач профессиональной деятельности на основе информационной и библиографической культуры с применением информационно-коммуникационных технологий и с учетом основных требований информационной безопасности
			ОПК-3.**ИД-2.** Планирует и выполняет практические действия в рамках компетенции	ОПК-3.2 Уметь: решать стандартные задачи профессиональной деятельности на основе информационной и библиографической культуры с применением информационно-коммуникационных технологий и с учетом основных требований информационной безопасности
			ОПК-3.**ИД-3.** Применяет методы анализа кой	ОПК-3.3 Иметь навыки: подготовки обзоров, аннотаций, составления

			деятельности и ее результатов в рамках практической компетенции	рефератов, научных докладов, публикаций и библиографии по научно-исследовательской работе с учетом требований информационной безопасности
	ПК-7	Способен обеспечивать информационную безопасность на уровне БД.	ПК-7.**ИД-1.** Сформирован понятийный аппарат и теоретическая основа для выполнения практических действий в рамках компетенции	ПК-7.1: освоение основных методов обеспечения информационную безопасность на уровне БД.
			ПК-7.**ИД-2.** Планирует и выполняет практические действия в рамках компетенции	ПК-7.2: навык самостоятельного обеспечения информационную безопасность на уровне БД.
			ПК-7.**ИД-3.** Применяет методы анализа кой деятельности и ее результатов в рамках практической компетенции	ПК-7.3: владение принципами и методами обеспечения информационную безопасность на уровне БД.
	ПК-11	Способен осуществлять администрирование процесса управления безопасностью сетевых	ПК-11.**ИД-1.** Сформирован понятийный аппарат и	ПК-11.1: освоение основных методов и средств

		устройств и программного обеспечения	теоретическая основа для выполнения практических действий в рамках компетенции	администрирования процесса управления безопасностью сетевых устройств и программного обеспечения
			ПК-11.**ИД-2.** Планирует и выполняет практические действия в рамках компетенции	ПК-11.2: навык самостоятельного администрирования процесса управления безопасностью сетевых устройств и программного обеспечения
			ПК-11.**ИД-3.** Применяет методы анализа кой деятельности и ее результатов в рамках практической компетенции	ПК-11.3: владение основными методами и средствами администрирования процесса управления безопасностью сетевых устройств и программного обеспечения

РАЗДЕЛ 2. СТРУКТУРА И СОДЕРЖАНИЕ ДИСЦИПЛИНЫ

2.1 Объем учебной дисциплины, включая контактную работу обучающегося с педагогическими работниками и самостоятельную работу обучающегося

Общая трудоемкость дисциплины, изучаемой в 5 семестре, составляет 6 зачетных единицы. По дисциплине предусмотрен *экзамен*.

Очная форма обучения

Вид учебной работы	**Всего часов**	**Семестры**				
		5				
Контактная работа обучающихся с педагогическими работниками (по видам учебных занятий) (всего):	**108**	**108**				
Учебные занятия лекционного типа	24	24				
Практические занятия	0	0				

Лабораторные занятия	36	36				
Контактная работа в ЭИОС и ИКР	48	48				
Самостоятельная работа обучающихся, всего	**81**	**81**				
Контроль промежуточной аттестации (час)	**27**	**экзам 27**				
ОБЪЕМ ДИСЦИПЛИНЫ В ЧАСАХ	**216**	**216**				

Заочная форма обучения

Вид учебной работы	**Всего часов**	**Семестры**				
		5	6			
Контактная работа обучающихся с педагогическими работниками (по видам учебных занятий) (всего):	**48**	**16**	**32**			
Учебные занятия лекционного типа	8	2	6			
Практические занятия	0	0	0			
Лабораторные занятия	16	6	10			
Контактная работа в ЭИОС и ИКР	24	8	16			
Самостоятельная работа обучающихся, всего	**159**	**56**	**103**			
Контроль промежуточной аттестации (час)	**9**		**экзам 9**			
ОБЪЕМ ДИСЦИПЛИНЫ В ЧАСАХ	**216**	**72**	**144**			

2.2. Учебно-тематический план учебной дисциплины

Очной формы обучения

Раздел, тема	**Виды учебной работы, академических часов**						
	Всего	**Самостоятельная работа**	**Контактная работа обучающихся с педагогическими работниками**				
			Всего	**Лекционные занятия**	**Семинарские/ практические занятия**	**Лабораторные занятия**	**Контактная работа в ЭИОС и ИКР**
Модуль 1 (семестр 5)							
Раздел 1 Особенности обеспечения ИБ РФ в различных сферах жизни	30	12	18	4	0	6	8

Раздел 2 Угрозы информационной безопасности	30	12	18	4	0	6	8
Раздел 3 Законодательный уровень информационной безопасности	30	12	18	4	0	6	8
Раздел 4 Построение системы информационной безопасности	30	12	18	4	0	6	8
Раздел 5 Защита информации в информационных системах и компьютерных сетях	30	12	18	4	0	6	8
Раздел 6 Обеспечение информационной безопасности	30	12	18	4	0	6	8
Контроль промежуточной аттестации (час)	**27**						
Общий объем, часов	**216**	**72**	**108**	**24**	**0**	**36**	**48**
Форма промежуточной аттестации	**экзамен**						
Общий объем часов по учебной дисциплине	**216**	**72**	**108**	**24**	**0**	**36**	**48**

Заочной формы обучения

Раздел, тема	**Виды учебной работы, академических часов**						
	Всего	**Самостоятельная работа**	**Контактная работа обучающихся с педагогическими работниками**				
			Всего	**Лекционные занятия**	**Семинарские/ практические занятия**	**Лабораторные занятия**	**Контактная работа в ЭИОС и ИКР**
Модуль 1 (семестр 5)							
Раздел 1.1	36	28	8	2	0	2	4
Раздел 1.2	36	28	8	0	0	4	4
Контроль промежуточной аттестации (час)	**0**						
Общий объем, часов	**72**	**56**	**16**	**2**	**0**	**6**	**8**

Форма промежуточной аттестации	

Модуль 2 (семестр 6)							
Раздел 2.1	33	25	8	2	0	2	4
Раздел 2.2	34	26	8	2	0	2	4
Раздел 2.3	34	26	8	2	0	2	4
Раздел 2.4	34	26	8	0	0	4	4
Контроль промежуточной аттестации (час)	**9**						
Общий объем, часов	**144**	**103**	**32**	**6**	**0**	**10**	**16**
Форма промежуточной аттестации	**экзамен**						
Общий объем часов по учебной дисциплине	**216**	**159**	**48**	**8**	**0**	**16**	**24**

РАЗДЕЛ 3. УЧЕБНО-МЕТОДИЧЕСКОЕ ОБЕСПЕЧЕНИЕ САМОСТОЯТЕЛЬНОЙ РАБОТЫ ОБУЧАЮЩИХСЯ ПО УЧЕБНОЙ ДИСЦИПЛИНЕ

3.1. Виды самостоятельной работы обучающихся по учебной дисциплине

Очной формы обучения

Раздел, тема	**Всего**	**Виды самостоятельной работы обучающихся**					
		Академическая активность, час	**Форма академической активности**	**Выполнение практ. заданий, час**	**Форма практического задания**	**Рубежный текущий контроль, час**	**Форма рубежного текущего контроля**
Модуль 1 (семестр 5)							
Раздел 1 Особенности обеспечения ИБ РФ в различных сферах жизни	12	5	Подготовка к лекционным и практическим занятиям, самостоятельное изучение раздела в ЭИОС	5	реферат	2	Компьютерное тестирование или иная форма рубежного контроля по усмотрению преподавателя
Раздел 2 Угрозы информационной безопасности	12	5	Подготовка к лекционным и практическим занятиям, самостоятельное изучение раздела в ЭИОС	5	реферат	2	Компьютерное тестирование или иная форма рубежного контроля по усмотрению преподавателя

Раздел 3 Законодательный уровень информационной безопасности	12	5	Подготовка к лекционным и практическим занятиям, самостоятельное изучение раздела в ЭИОС	5	реферат	2	Компьютерное тестирование или иная форма рубежного контроля по усмотрению преподавателя
Раздел 4 Построение системы информационной безопасности	12	5	Подготовка к лекционным и практическим занятиям, самостоятельное изучение раздела в ЭИОС	5	реферат	2	Компьютерное тестирование или иная форма рубежного контроля по усмотрению преподавателя
Раздел 5 Защита информации в информационных системах и компьютерных сетях	12	5	Подготовка к лекционным и практическим занятиям, самостоятельное изучение раздела в ЭИОС	5	реферат	2	Компьютерное тестирование или иная форма рубежного контроля по усмотрению преподавателя
Раздел 6 Обеспечение информационной безопасности	12	5	Подготовка к лекционным и практическим занятиям, самостоятельное изучение раздела в ЭИОС	5	реферат	2	Компьютерное тестирование или иная форма рубежного контроля по усмотрению преподавателя
Общий объем по модулю/семестру, часов	**72**	**30**		**30**		**12**	
Общий объем по дисциплине, часов	**72**	**30**		**30**		**12**	

Заочной формы обучения

Раздел, тема	**Всего**	**Виды самостоятельной работы обучающихся**					
		Академическая активность, час	**Форма академической активности**	**Выполнение практ. заданий, час**	**Форма практического задания**	**Рубежный текущий контроль, час**	**Форма рубежного текущего контроля**
Модуль 1 (семестр 5)							
Раздел 1.1	28	13	Подготовка к лекционным и практическим занятиям, самостоятельное изучение раздела в ЭИОС	13	реферат	2	Компьютерное тестирование или иная форма рубежного контроля по усмотрению преподавателя

Раздел 1.2	28	13	Подготовка к лекционным и практическим занятиям, самостоятельное изучение раздела в ЭИОС	13	реферат	2	Компьютерное тестирование или иная форма рубежного контроля по усмотрению преподавателя
Общий объем по модулю/семестру, часов	**56**	**26**		**26**		**4**	
Модуль 2 (семестр 6)							
Раздел 2.1	25	11	Подготовка к лекционным и практическим занятиям, самостоятельное изучение раздела в ЭИОС	12	реферат	2	Компьютерное тестирование или иная форма рубежного контроля по усмотрению преподавателя
Раздел 2.2	26	12	Подготовка к лекционным и практическим занятиям, самостоятельное изучение раздела в ЭИОС	12	реферат	2	Компьютерное тестирование или иная форма рубежного контроля по усмотрению преподавателя
Раздел 2.3	26	12	Подготовка к лекционным и практическим занятиям, самостоятельное изучение раздела в ЭИОС	12	реферат	2	Компьютерное тестирование или иная форма рубежного контроля по усмотрению преподавателя
Раздел 2.4	26	12	Подготовка к лекционным и практическим занятиям, самостоятельное изучение раздела в ЭИОС	12	реферат	2	Компьютерное тестирование или иная форма рубежного контроля по усмотрению преподавателя
Общий объем по модулю/семестру, часов	**103**	**47**		**48**		**8**	
Общий объем по дисциплине, часов	**159**	**73**		**74**		**12**	

3.2 Методические указания к самостоятельной работе по учебной дисциплине

РАЗДЕЛ 1 Особенности обеспечения информационной безопасности РФ в различных сферах жизни

Перечень изучаемых элементов содержания

Место информационной безопасности в национальной безопасности РФ.

Цели и задачи обеспечения информационной безопасности.

Составляющие информационной безопасности.

Виды и источники угроз информационной безопасности РФ.

Структура государственной системы обеспечения информационной безопасности РФ.

Основные объекты обеспечения информационной безопасности РФ в общегосударственных информационных и телекоммуникационных системах.

Вопросы для самоподготовки:

1. Экономическая и информационная безопасность
2. Доктрина информационной безопасности РФ
3. Основные составляющие информационной безопасности
4. Ключевые вопросы информационной безопасности
5. Понятие информационного пространства
6. Понятие информационной безопасности
7. Субъекты и объекты информационной безопасности
8. Нормативно-правовые основы информационной безопасности
9. Понятие экономической информации

Практическое задание к разделу 1

Форма практического задания: лабораторная работа по использованию Интернет-ресурсов для оценки воздействия ИКТ-технологий на неприкосновенность частной жизни

Цель занятия: формирование ответственного отношения к информационной деятельности, связанной с обработкой и хранением информации; приобретение опыта профилактической и предупреждающей деятельности по отношению к информационным угрозам на уровне личной информационной безопасности.

Для выполнения лабораторной работы студенты разбиваются на пары и выполняют задания:

1) найти как можно больше личной информации о коллеге, используя общедоступные сетевые ресурсы.
2) оценить возможность использования найденной информации злоумышленниками, например:
   - телефонными террористами
   - мошенниками
   - похитителями номеров банковских карт
   - распространителями рекламной продукции и т.д.
3) Передать собранные материалы "коллеге" и получить досье с информацией о себе
4) Оценить уровень конфиденциальности, актуальности и достоверности собранной информации
5) Проанализировать выводы коллеги о возможности использования найденной информации злоумышленниками
6) Оценить уровень влияния цифровых технологий на свою частную жизнь и продумать шаги по обеспечению желаемого уровня безопасности

Контрольные вопросы:

1. Основные понятия информатизации общества и информационной безопасности
2. Цели и задачи обеспечения информационной безопасности
3. Место информационной безопасности в национальной безопасности РФ.

4. Виды и источники угроз информационной безопасности РФ.
5. Структура государственной системы обеспечения информационной безопасности РФ.
6. Понятие и особенности экономической информации как объекта безопасности

Рубежный контроль к разделу 1: форма рубежного контроля – отчет по лабораторной работе.

Раздел 2 Угрозы информационной безопасности

Перечень изучаемых элементов содержания

1. Виды угроз информационной безопасности
2. Классификация источников угроз
3. Основные виды защищаемой информации

Вопросы для самоподготовки:

1. Действия и события, нарушающие информационную безопасность
2. Основные виды каналов утечки информации
3. Пути несанкционированного доступа к информации
4. Стратегия и тактика злоумышленника при несанкционированном доступе
5. Личностно-профессиональные характеристики сотрудников, способствующие реализации информационных угроз
6. Признаки воздействия вирусов на компьютерную систему

Практическое задание к разделу 2

Форма практического задания: лабораторная работа «Обеспечение безопасности операционных систем семейства Windows»

Цель: изучить архитектуру и базовые средства обеспечения безопасности на примере Windows 7; научится управлять пользователями (учетными записями) в компьютере; научится разграничивать доступ к файлам и каталогам.

Рубежный контроль к разделу 2: форма рубежного контроля – отчет по лабораторной работе

Контрольные вопросы:

1. Классификация угроз безопасности
2. Угрозы нарушения конфиденциальности
3. Угрозы нарушения целостности информации.
4. Угрозы нарушения работоспособности (отказ в обслуживании)
5. Уязвимости компьютерной системы
6. Классификация атак на компьютерную систему
7. Вредоносное программное обеспечение

РАЗДЕЛ 3 ЗАКОНОДАТЕЛЬНЫЙ УРОВЕНЬ ИНФОРМАЦИОННОЙ БЕЗОПАСНОСТИ

Перечень изучаемых элементов содержания

Закон " Об информации, информационных технологиях и о защите информации"

Закон «О государственной тайне»

Закон «О коммерческой тайне»

Закон «О персональных данных»

Вопросы для самоподготовки:

1. Понятие информационной войны и информационной преступности
2. Статьи Уголовного кодекса о компьютерных преступлениях
3. Обзор законодательства США в области информационной безопасности
4. Обзор законодательства европейских стран в области информационной безопасности

ПРАКТИЧЕСКОЕ ЗАДАНИЕ К РАЗДЕЛУ 3

Форма практического задания: лабораторная работа «Правовое обеспечении информационной безопасности»

Цель: анализ основных законодательных актов РФ в области ИБ

1) Конституция РФ: статьи 23, 24, 29, 41, 42 2.
2) Закон «Об информации, информационных технологиях и о защите информации» (статья 15)
3) Закон «Об информации, информационных технологиях и о защите информации» (статья 16)
4) Закон «О государственной тайне»
5) Закон «О персональных данных»
6) Закон «О лицензировании отдельных видов деятельности»
7) Закон «Об электронной цифровой подписи»
8) Уголовный кодекс РФ: статьи 138, 183, 272, 273, 274

Задание: ознакомиться с законодательным актом, ответить на вопросы:

1) Когда был принят закон, когда была принята последняя редакция закона?
2) Какие основные понятия рассматриваются в законе?
3) Как отражены в законе основные аспекты информационной безопасности:
   - доступность,
   - целостность
   - конфиденциальность?
4) Какие предусмотрены в законе

- меры ограничительной направленности (т.е. меры, направленные на создание и поддержание в обществе негативного (в том числе с применением наказаний) отношения к нарушениям и нарушителям информационной безопасности);

- направляющие и координирующие меры (т.е. меры созидательной направленности, способствующие повышению образованности общества в области информационной безопасности, помогающие в разработке и распространении средств обеспечения информационной безопасности).

5) Как в законе учтено современное состояние информационных технологий?

Контрольные вопросы:

1. Основные законодательные акты РФ в области информационной безопасности
2. Перечень сведений, относящихся к коммерческой тайне. Перечень сведений, которые не могут составлять коммерческую тайну
3. Объекты банковской тайны
4. Меры ограничительной направленности по отношению к нарушениям и нарушителям информационной безопасности

РУБЕЖНЫЙ КОНТРОЛЬ К РАЗДЕЛУ 3: форма рубежного контроля – отчет по лабораторной работе

РАЗДЕЛ 4 ПОСТРОЕНИЕ СИСТЕМЫ ИНФОРМАЦИОННОЙ БЕЗОПАСНОСТИ

Перечень изучаемых элементов содержания

Основные аспекты построения системы информационной безопасности

Программа информационной безопасности

Модели информационной безопасности

Требования и основные этапы реализации информационной безопасности

Мероприятия по защите информации

Анализ и управление рисками информационной безопасности

Вопросы для самоподготовки:

1. Модели информационной безопасности
2. Разработка многоуровневой политики информационной безопасности
3. Основные этапы реализации информационной безопасности
4. Рентабельность системы защиты информации
5. Анализ информационных рисков, угроз и уязвимостей системы.
6. Управление рисками на различных стадиях жизненного цикла информационной системы.
7. Трехмерная модель “куб безопасности”.
8. Оценка рисков

9. Программное обеспечение для анализа рисков информационной безопасности

ПРАКТИЧЕСКОЕ ЗАДАНИЕ К РАЗДЕЛУ 4

Форма практического задания: лабораторная работа по оценке экономической эффективности внедрения системы защиты информации

Цель работы: изучить методику экономической оценки эффективности системы защиты информации, получить навыки обоснования целесообразности внедрения системы по обеспечению информационной безопасности на предприятии с экономической точки зрения

Описание ситуации

Компании требуется оценить проект по защите одного из сегментов сети своей информационной системы при помощи системы анализа защищенности. Известны:

величина риска, исчисляемая в денежном выражении, которая учитывает потери от реализации тех или иных атак и вероятности их осуществления;

стоимость внедряемого программного комплекса;

на сколько процентов сократится величина риска после внедрения разработанного программного комплекса.

Оценка экономической эффективности внедрения системы защиты информации

Для оценки инвестиционного проекта применяется метод дисконтирования денежных потоков

Контрольные вопросы:

1. Понятие и функции системы защиты информации
2. Общие принципы обеспечения информационной безопасности
3. Специальные принципы обеспечения информационной безопасности
4. Обеспечивающие подсистемы защиты информации

Рубежный контроль к разделу 4: форма рубежного контроля – отчет по лабораторной работе.

РАЗДЕЛ 5 ЗАЩИТА ИНФОРМАЦИИ В ИНФОРМАЦИОННЫХ СИСТЕМАХ И КОМПЬЮТЕРНЫХ СЕТЯХ

Перечень изучаемых элементов содержания

Анализ защищенности информационных систем

Криптографические методы защиты информации

Программно-аппаратные средства защиты информации

Защита информации в компьютерных сетях

Вопросы для самоподготовки:

1. Основные аспекты криптоанализа
2. Обеспечение безопасности беспроводных сетей
3. Обеспечение безопасности электронной почты

4. Безопасность при использовании облачных сервисов
5. Типовые удаленные атаки в глобальных сетях и механизмы их реализации
6. Особенности защиты мультимедийного контента в телекоммуникационных сетях.
7. Возможности и особенности сетевых вредоносных программ.

ПРАКТИЧЕСКОЕ ЗАДАНИЕ К РАЗДЕЛУ 5

Форма практического задания: Лабораторная работа по изучению программных продуктов защиты информации на примере программы PGP (PrettyGoodPrivacy)

Цель работы: освоение средств программной системы PGP для шифрования конфиденциальных ресурсов и разграничения доступа к ним, обеспечение целостности информационных ресурсов с помощью механизма электронной цифровой подписи

Контрольные вопросы:
1. Программно-аппаратные средства защиты информации
2. Симметричные методы шифрования
3. Алгоритмы криптографического преобразования данных DES, AES 31.
4. Алгоритм криптографического преобразования данных ГОСТ 28147
5. Шифрование с открытым ключом
6. Механизм электронной цифровой подписи
7. Вредоносное программное обеспечение
8. Антивирусная защита компьютерных систем

Рубежный контроль к разделу 5: форма рубежного контроля – отчет по лабораторной работе

РАЗДЕЛ 6 ОБЕСПЕЧЕНИЕ ИНФОРМАЦИОННОЙ БЕЗОПАСНОСТИ

Перечень изучаемых элементов содержания

Требования к архитектуре информационной системы для обеспечения безопасности ее функционирования

Стандартизация подходов к обеспечению информационной безопасности

Защищенный электронный документооборот.

Вопросы для самоподготовки:
1. Обеспечение информационной безопасности автоматизированных банковских систем
2. Информационная безопасность электронной коммерции
3. Обеспечение компьютерной безопасности учетной информации
4. Информационная безопасность предпринимательской деятельности
5. Методика защиты электронной почты
6. Обеспечение информационной безопасности должностных лиц и представителей деловых кругов
7. Виды несанкционированного копирования компьютерной информации.
8. Информационная безопасность пользователей мобильных устройств

Практическое задание к разделу 6

Форма практического задания: лабораторная работа «Защита электронных документов с помощью ЦВЗ»

Цель работы: изучение методов защиты электронных документов с использованием цифровых водяных знаков.

Контрольные вопросы:

1. Протоколирование и аудит информационной безопасности
2. Защищенный электронный документооборот
3. Оценочные стандарты и технические спецификации.
4. "Оранжевая книга" как оценочный стандарт
5. Критерии оценки безопасности информационных технологий. ГОСТ Р ИСО/МЭК 15408-1-2012

Рубежный контроль к разделу 6: форма рубежного контроля – отчет по лабораторной работе

РАЗДЕЛ 4. ФОНД ОЦЕНОЧНЫХ СРЕДСТВ ДЛЯ ПРОВЕДЕНИЯ ПРОМЕЖУТОЧНОЙ АТТЕСТАЦИИ ОБУЧАЮЩИХСЯ ПО УЧЕБНОЙ ДИСЦИПЛИНЕ

4.1. Форма промежуточной аттестации обучающегося по учебной дисциплине

Контрольным мероприятием промежуточной аттестации обучающихся по учебной дисциплине является **экзамен и зачет,** который проводится в**устной** форме.

4.2. Перечень компетенций с указанием этапов их формирования в процессе освоения образовательной программы

ОПК-3; ПК-7; ПК-11

Код компетенции	Содержание компетенции (части компетенции)	Результаты обучения	Этапы формирования компетенций в процессе освоения образовательной программы
ОПК-3	Способен решать стандартные задачи профессиональной деятельности на основе информационной и библиографической культуры с применением информационно-коммуникационных технологий и с учетом основных требований	ОПК-3.1 Знать: принципы, методы и средства решения стандартных задач профессиональной деятельности на основе информационной и библиографической культуры с применением информационно-коммуникационных технологий и с учетом основных требований информационной безопасности	Этап формирования знаний

	информационной безопасности;	ОПК-3.2 Уметь: решать стандартные задачи профессиональной деятельности на основе информационной и библиографической культуры с применением информационно-коммуникационных технологий и с учетом основных требований информационной безопасности	Этап формирования умений
		ОПК-3.3 Иметь навыки: подготовки обзоров, аннотаций, составления рефератов, научных докладов, публикаций и библиографии по научно-исследовательской работе с учетом требований информационной безопасности	Этап формирования навыков и получения опыта
ПК-7	Способен	ПК-7.1: освоение основных	Этап формирования
	обеспечивать информационную безопасность на уровне БД.	методов обеспечения информационную безопасность на уровне БД.	умений
		ПК-7.2: навык самостоятельного обеспечения информационную безопасность на уровне БД.	Этап формирования умений
		ПК-7.3: владение принципами и методами обеспечения информационную безопасность на уровне БД.	Этап формирования навыков и получения опыта
ПК-11	Способен осуществлять администрирование процесса управления безопасностью сетевых устройств и программного обеспечения	ПК-11.1: освоение основных методов и средств администрирования процесса управления безопасностью сетевых устройств и программного обеспечения	Этап формирования знаний
		ПК-11.2: навык самостоятельного администрирования процесса	Этап формирования умений

		управления безопасностью сетевых устройств и программного обеспечения	
		ПК-11.3: владение основными методами и средствами администрирования процесса управления безопасностью сетевых устройств и программного обеспечения	Этап формирования навыков и получения опыта

4.3Описание показателей и критериев оценивания компетенций на различных этапах их формирования, описание шкал оценивания

Код компетенции	Этапы формирования компетенций	Показатель оценивания компетенции	Критерии и шкалы оценивания
ОПК-3; ПК-7; ПК-11	Этап формирования знаний.	Теоретический блок вопросов. Уровень освоения программного материала, логика и грамотность изложения, умение самостоятельно обобщать и излагать	1) обучающийся глубоко и прочно освоил программный материал, исчерпывающе, последовательно, грамотно и логически стройно его излагает, тесно увязывает с задачами и будущей деятельностью, не затрудняется с ответом при видоизменении задания, умеет самостоятельно

		материал	обобщать и излагать материал, не допуская ошибок: (9-10] баллов; 2) обучающийся твердо знает программный материал, грамотно и по существу излагает его, не допуская существенных неточностей в ответе на вопрос, может правильно применять теоретические положения: [8-9) баллов; 3) обучающийся освоил основной материал, но не знает отдельных деталей, допускает неточности, недостаточно правильные формулировки, нарушает последовательность в изложении программного материала: (6-8) баллов; 4) обучающийся не знает значительной части программного материала, допускает существенные ошибки: [0-6] баллов.
ОПК-3; ПК-7; ПК-11	Этап формирования умений	Аналитическое задание *(задачи, ситуационные задания, кейсы, проблемные ситуации и т.д.)* Практическое применение теоретических положений применительно к профессиональным задачам, обоснование принятых решений	1) свободно справляется с задачами и практическими заданиями, правильно обосновывает принятые решения, задание выполнено верно, даны ясные аналитические выводы к решению задания, подкрепленные теорией: (9-10] баллов; 2) владеет необходимыми умениями и навыками при выполнении практических заданий, задание выполнено верно, отмечается хорошее развитие аргумента, однако отмечены погрешности в ответе, скорректированные при собеседовании: [8-9) баллов; 3) испытывает затруднения в выполнении практических заданий, задание выполнено с ошибками, отсутствуют логические выводы и заключения к решению: (6-8) баллов; 4) практические задания,
ОПК-3; ПК-7; ПК-11	Этап формирования навыков и получения опыта.	Аналитическое задание *(задачи, ситуационные задания, кейсы, проблемные ситуации и т.д.)*	

		Решение практических заданий и задач, владение навыками и умениями при выполнении практических заданий, самостоятельность, умение обобщать и излагать материал.	задачи выполняет с большими затруднениями или задание не выполнено вообще, или задание выполнено не до конца, нет четких выводов и заключений по решению задания, сделаны неверные выводы по решению задания: [0-6] баллов.

4.4 Типовые контрольные задания или иные материалы, необходимые для оценки знаний, умений, навыков и (или) опыта деятельности, характеризующих этапы формирования компетенций в процессе освоения образовательной программы

Примерные вопросы для проведения промежуточной аттестации обучающихся по учебной дисциплине

Теоретический блок вопросов:

1. Понятие информации. Фазы обращения информации в информационных системах.
2. Место информационной безопасности в национальной безопасности РФ.
3. Виды и источники угроз информационной безопасности РФ.
4. Структура государственной системы обеспечения информационной безопасности РФ.
5. Организация технической защиты информации в РФ.
6. Цели и задачи обеспечения информационной безопасности.
7. Архитектура СЗИ организации и основные требования к средствам защиты.
8. Функциональное построение СЗИ организации и назначение основных подразделений.
9. Элементарные модели СЗИ организации. Семирубежная модель защиты.
10. Последовательность и содержание основных этапов проектирования СЗИ организации.
11. Содержание процесса эксплуатации СЗИ организации.
12. Анализ угроз информационной безопасности.
13. Внутренние и внешние источники угроз информационной безопасности. Схема воздействия угроз на информационную систему.
14. Управление рисками на различных стадиях жизненного цикла информационной системы.
15. Трехмерная модель *“куб безопасности”.*
16. Перечень основных формальных и неформальных средств защиты информации.
17. Стратегии защиты информации на объекте информатизации.
18. Анализ информационных рисков, угроз и уязвимостей системы. Оценка рисков по двум факторам.
19. Анализ информационных рисков, угроз и уязвимостей системы. Оценка рисков по трем факторам.
20. Роль персонала в обеспечении информационной безопасности предприятия.
21. Криптографическая защита информации. Классические криптоалгоритмы - моноалфавитные подстановки.
22. Криптографическая защита информации. Классические криптоалгоритмы - многоалфавитные подстановки.
23. Криптографическая защита информации. Классические криптоалгоритмы - перестановки.
24. Шифрование методом гаммирования.

25. Современные симметричные системы шифрования. Обобщенная схема симметричного шифрования.
26. Симметричная система шифрования DES.
27. Отечественный стандарт симметричного шифрования ГОСТ 28147-89.
28. Современные асимметричные системы шифрования. Обобщенная схема асимметричного шифрования.
29. Асимметричная система шифрования RSA.
30. Электронная цифровая подпись. Обобщенная схема постановки и проверки ЭЦП.
31. Отечественный стандарт цифровой подписи ГОСТ Р34.10-94 (ГОСТ Р34.10-2001).
32. Стеганографические методы защиты информации. Обобщенная модель стегосистемы.
33. Классификация современных стеганографических методов защиты информации.
34. Цифровые водяные знаки. Области применения и особенности аутентификации сообщений с использованием ЦВЗ.
35. Политики безопасности компьютерных систем.
36. Современные методы и средства обеспечения сетевой безопасности.
37. Вредоносное программное обеспечение и методы борьбы с ним.
38. Методологические и практические проблемы обеспечения информационной безопасности в современном обществе.

4.5Методические материалы, определяющие процедуры оценивания знаний, умений, навыков и (или) опыта деятельности, характеризующих этапы формирования компетенций

Промежуточная аттестация по учебной дисциплине проводится в соответствии с Положением о промежуточной аттестации обучающихся по основным профессиональным образовательным программам высшего образования – программ бакалаврита в Институте государственного администрирования и Положение о балльно-рейтинговой системе оценки успеваемости обучающихся по основным профессиональным образовательным программам высшего образования - программам бакалавриата в Институте государственного администрирования.

На промежуточную аттестацию отводится 20 рейтинговых баллов.

Ответы обучающегося на контрольном мероприятии промежуточной аттестации оцениваются педагогическим работником по 20 - балльной шкале, а итоговая оценка по учебной дисциплине выставляется по пятибалльной системе для экзамена/дифференцированного зачета и по системе зачтено/не зачтено для зачета.

Критерии выставления оценки определяются Положением о балльно-рейтинговой системе оценки успеваемости обучающихся по основным профессиональным образовательным программам высшего образования - программам бакалавриата в Институте государственного администрирования.

РАЗДЕЛ 5. УСЛОВИЯ РЕАЛИЗАЦИИ ДИСЦИПЛИНЫ

5.1. Перечень основной и дополнительной учебной литературы для освоения учебной дисциплины

1. Суворова, Г. М. Информационная безопасность : учебное пособие для вузов / Г. М. Суворова. — Москва : Издательство Юрайт, 2022. — 253 с. — (Высшее образование). — ISBN 978-5-534-13960-0. — Текст : электронный //

Образовательная платформа Юрайт [сайт]. — URL: https://urait.ru/bcode/496741 (дата обращения: 16.05.2022).
2. Внуков, А. А. Защита информации : учебное пособие для вузов / А. А. Внуков. — 3-е изд., перераб. и доп. — Москва : Издательство Юрайт, 2022. — 161 с. — (Высшее образование). — ISBN 978-5-534-07248-8. — Текст : электронный // Образовательная платформа Юрайт [сайт]. — URL: https://urait.ru/bcode/490277 (дата обращения: 09.04.2022).

5.1.2. Дополнительная литература

1. Щеглов, А. Ю. Защита информации: основы теории : учебник для вузов / А. Ю. Щеглов, К. А. Щеглов. — Москва : Издательство Юрайт, 2022. — 309 с. — (Высшее образование). — ISBN 978-5-534-04732-5. — Текст : электронный // Образовательная платформа Юрайт [сайт]. — URL: https://www.urait.ru/bcode/490019 (дата обращения: 12.04.2022).

2. Казарин, О. В. Надежность и безопасность программного обеспечения : учебное пособие для вузов / О. В. Казарин, И. Б. Шубинский. — Москва : Издательство Юрайт, 2022. — 342 с. — (Высшее образование). — ISBN 978-5-534- 05142-1. — Текст : электронный // Образовательная платформа Юрайт [сайт]. — URL: https://urait.ru/bcode/493262 (дата обращения: 09.04.2022).

5.2 Перечень ресурсов информационно-коммуникационной сети «Интернет», необходимых для освоения учебной дисциплины

№ №	Название электронного ресурса	Описание электронного ресурса	Используемый для работы адрес
1.	ЭБС «Университетская библиотека онлайн»	Электронная библиотека, обеспечивающая доступ высших и средних учебных заведений, публичных библиотек и корпоративных пользователей к наиболее востребованным материалам по всем отраслям знаний от ведущих российских	http://biblioclub.ru/
		издательств	
2.	Научная электронная библиотека eLIBRARY.ru	Крупнейший российский информационно-аналитический портал в области науки, технологии, медицины и образования, содержащий рефераты и полные тексты более 34 млн научных публикаций и патентов	http://elibrary.ru/
3.	Образовательная платформа Юрайт	Электронно-библиотечная система для ВУЗов, ССУЗов, обеспечивающая доступ к учебникам, учебной и методической литературе по различным дисциплинам.	https://urait.ru/

4.	База данных "EastView"	Полнотекстовая база данных периодических изданий	https://dlib.eastview.com
5.	Электронная библиотека "Grebennikon"	Библиотека предоставляет доступ более чем к 30 журналам, выпускаемых Издательским домом "Гребенников".	https://grebennikon.ru/

5.3 Методические указания для обучающихся по освоению учебной дисциплины

Освоение обучающимся учебной дисциплины «*Информационная безопасность*» предполагает изучение материалов дисциплины на аудиторных занятиях и в ходе самостоятельной работы. Аудиторные занятия проходят в форме лекций, семинаров и практических занятий. Самостоятельная работа включает разнообразный комплекс видов и форм работы обучающихся.

Для успешного освоения учебной дисциплины и достижения поставленных целей необходимо внимательно ознакомиться с рабочей программы учебной дисциплины, доступной в электронной информационно-образовательной среде ЧУ ВО «ИГА».

Следует обратить внимание на списки основной и дополнительной литературы, на предлагаемые преподавателем ресурсы информационно-телекоммуникационной сети Интернет. Эта информация необходима для самостоятельной работы обучающегося.

При подготовке к аудиторным занятиям необходимо помнить особенности каждой формы его проведения.

Подготовка к учебному занятию лекционного типа заключается в следующем.

С целью обеспечения успешного обучения обучающийся должен готовиться к лекции, поскольку она является важнейшей формой организации учебного процесса, поскольку:

− знакомит с новым учебным материалом;

− разъясняет учебные элементы, трудные для понимания;

− систематизирует учебный материал;

− ориентирует в учебном процессе.

С этой целью:

− внимательно прочитайте материал предыдущей лекции;

− ознакомьтесь с учебным материалом по учебнику и учебным пособиям с темой прочитанной лекции;

− внесите дополнения к полученным ранее знаниям по теме лекции на полях лекционной тетради;

− запишите возможные вопросы, которые вы зададите лектору на лекции по материалу изученной лекции;

− постарайтесь уяснить место изучаемой темы в своей подготовке;

− узнайте тему предстоящей лекции (по тематическому плану, по информации лектора) и запишите информацию, которой вы владеете по данному вопросу.

Подготовка к занятию семинарского типа

При подготовке и работе во время проведения лабораторных работ и занятий семинарского типа следует обратить внимание на следующие моменты: на процесс предварительной подготовки, на работу во время занятия, обработку полученных результатов, исправление полученных замечаний.

Предварительная подготовка к учебному занятию семинарского типа заключается в изучении теоретического материала в отведенное для самостоятельной работы время, ознакомление с инструктивными материалами с целью осознания задач лабораторной работы/практического занятия, техники безопасности при работе с приборами, веществами.

Работа во время проведения учебного занятия семинарского типа включает:

− консультирование студентов преподавателями и вспомогательным персоналом с целью предоставления исчерпывающей информации, необходимой для самостоятельного выполнения предложенных преподавателем задач, ознакомление с правилами техники безопасности при работе в лаборатории;

− самостоятельное выполнение заданий согласно обозначенной учебной программой тематики.

Обработка, обобщение полученных результатов лабораторной работы проводиться обучающимися самостоятельно или под руководством преподавателя (в зависимости от степени сложности поставленных задач). В результате оформляется индивидуальный отчет. Подготовленная к сдаче на контроль и оценку работа сдается преподавателю. Форма отчетности может быть письменная, устная или две одновременно. Главным результатом в данном случае служит получение положительной оценки по каждой лабораторной работе/практическому занятию. Это является необходимым условием при проведении рубежного контроля и допуска к зачету/дифференцированному зачету/экзамену. При получении неудовлетворительных результатов обучающийся имеет право в дополнительное время пересдать преподавателю работу до проведения промежуточной аттестации.

Самостоятельная работа.

Для более углубленного изучения темы задания для самостоятельной работы рекомендуется выполнять параллельно с изучением данной темы. При выполнении заданий по возможности используйте наглядное представление материала. Более подробная информация о самостоятельной работе представлена в разделах «Учебно-методическое обеспечение самостоятельной работы по дисциплине (модулю)», «Методические указания к самостоятельной работе по дисциплине (модулю»).

5.4 Информационно-технологическое обеспечение образовательного процесса по учебной дисциплине

5.4.1. Средства информационных технологий

1. Персональные компьютеры;
2. Средства доступа к Интернет;
3. Проектор;
4. Принтер.

5.4.2. Программное обеспечение

1. Microsoft® Office Professional Plus 2007 Russian Academic OPEN No Level
2. Adobe Photoshop Extended CS4 11.0 WIN AOO License RU
3. Операционная система Windows 7
4. Microsoft Office Professional Plus 2007 Russian Academic OPEN No Level
5. Справочно-правовая система Консультант+
6. Acrobat Reader DC
7. 7-Zip
8. SKYDNS
9. TrueConf(client)

5.4.3. Информационные справочные системы и профессиональные базы данных

№ №	Название электронного ресурса	Описание электронного ресурса	Используемый для работы адрес
1.	ЭБС «Университетская библиотека онлайн»	Электронная библиотека, обеспечивающая доступ высших и средних учебных заведений, публичных библиотек и корпоративных пользователей к наиболее востребованным материалам по всем отраслям знаний от ведущих российских издательств	http://biblioclub.ru/
2.	Научная электронная библиотека eLIBRARY.ru	Крупнейший российский информационно-аналитический портал в области науки, технологии, медицины и образования, содержащий рефераты и полные тексты более 34 млн научных публикаций и патентов	http://elibrary.ru/
3.	Образовательная платформа Юрайт	Электронно-библиотечная система для ВУЗов, ССУЗов, обеспечивающая доступ к учебникам, учебной и методической литературе по различным дисциплинам.	https://urait.ru/
4.	База данных "EastView"	Полнотекстовая база данных периодических изданий	https://dlib.eastview.com
5.	Электронная библиотека "Grebennikon"	Библиотека предоставляет доступ более чем к 30 журналам, выпускаемых Издательским домом "Гребенников".	https://grebennikon.ru/

5.5 Материально-техническое обеспечение образовательного процесса по учебной дисциплине

Для изучения учебной дисциплины *«Информационная безопасность»* в рамках реализации основной профессиональной образовательной программы высшего образования – программы бакалаврита по направлению подготовки/специальности 09.03.01 «Информатика и вычислительная техника» очной, заочной формы обучения *и*спользуются:

Учебная аудитория для занятий лекционного типа оснащена специализированной мебелью (стол для преподавателя, парты, стулья, доска для написания мелом); техническими средствами обучения (видеопроекционное оборудование, средства звуковоспроизведения, экран и имеющие выход в сеть Интернет), а также (при наличии) демонстрационными печатными пособиями.

Учебная аудитория для занятий семинарского типа: оснащена специализированной мебелью (стол для преподавателя, парты, стулья, доска для написания мелом); техническими средствами обучения (видеопроекционное оборудование, средства звуковоспроизведения, экран и имеющие выход в сеть Интернет), а также (при наличии) демонстрационными печатными пособиями.

По теме с 1 по 6 проводятся лабораторные занятия в **Лаборатории информационных технологий и обеспечения информационной безопасности,** оснащенной специализированной мебелью (стол для преподавателя, парты, стулья, доска для написания мелом); техническими средствами обучения (видеопроекционное оборудование, средства звуковоспроизведения, экран и имеющие выход в сеть Интернет), а также специализированным лабораторным оборудованием.

Помещения для самостоятельной работы обучающихся: оснащены специализированной мебелью (парты, стулья) техническими средствами обучения (персональные компьютеры с доступом в сеть Интернет и обеспечением доступа в электронно-информационную среду института, программным обеспечением).

5.6 Образовательные технологии

При реализации учебной дисциплины *«Информационная безопасность»* применяются различные образовательные технологии, в том числе технологии электронного обучения.

Освоение учебной дисциплины *«Информационная безопасность»* предусматривает использование в учебном процессе активных и интерактивных форм проведения учебных занятий в форме компьютерных симуляций, деловых и ролевых игр, разбор конкретных ситуаций в сочетании с внеаудиторной работой с целью формирования и развития **профессиональных** навыков обучающихся.

Учебные часы дисциплины *«Информационная безопасность»* предусматривают классическую контактную работу преподавателя с обучающимся в аудитории и контактную работу посредством электронной информационно-образовательной среды в синхронном и асинхронном режиме (вне аудитории) посредством применения возможностей компьютерных технологий (электронная почта, электронный учебник, тестирование, вебинар, видеофильм, презентация, форум и др.).

В рамках учебной дисциплины *«Информационная безопасность»* предусмотрены встречи с руководителями и работниками организаций, деятельность которых связана с *направленностью*, реализуемой основной профессиональной образовательной программы высшего образования – программы бакалавриата.

ЛИСТ РЕГИСТРАЦИИ ИЗМЕНЕНИЙ

№ п/п	Содержание изменения	Реквизиты документа об утверждении изменения	Дата введения изменения
1.			
2.			