Образовательное частное учреждение высшего образования

«МОСКОВСКИЙ УНИВЕРСИТЕТ ИМЕНИ А.С. ГРИБОЕДОВА»

(ИМПЭ им. А.С. Грибоедова)

Институт международной экономики, лидерства и менеджмента

УТВЕРЖДАЮ
Директор института
международной экономики,
лидерства и менеджмента
_____ А.А. Панарин
«28» сентября 2023 г.

Рабочая программа дисциплины
ИНФОРМАЦИОННАЯ БЕЗОПАСНОСТЬ

Направление подготовки 09.03.03 Прикладная информатика
(уровень бакалавриат)

Направленность (профиль):
«Анализ данных»

Форма обучения: очная

Москва

Рабочая программа дисциплины «Информационная безопасность». Направление подготовки 09.03.03 Прикладная информатика, направленность (профиль): «Анализ данных» / А.А. Шестемиров – М.: ИМПЭ им. А.С. Грибоедова. – 26 с.

Рабочая программа дисциплины составлена на основании федерального государственного образовательного стандарта высшего образования – бакалавриат по направлению подготовки 09.03.03 Прикладная информатика, утвержденного приказом Министерства образования и науки Российской Федерации от «19» сентября 2017 № 922 (с изменениями и дополнениями) и Профессионального стандарта «Программист», утвержденного приказом Министерства труда и социальной защиты Российской Федерации от 18 ноября 2013 г. № 679н (зарегистрирован Министерством юстиции Российской Федерации 18 декабря 2013 г., регистрационный № 30635), с изменением, внесенным приказом Министерства труда и социальной защиты Российской Федерации от 12 декабря 2016 г. № 727н (зарегистрирован Министерством юстиции Российской Федерации 13 января 2017 г., регистрационный № 45230), Профессионального стандарта «Специалист по ин-формационным системам», утвержденный приказом Министерства труда и социальной защиты Российской Федерации от 18 ноября 2014 г. № 896н (зарегистрирован Министерством юстиции Российской Федерации 24 декабря 2014 г., регистрационный № 35361), с изменением, внесенным приказом Министерства труда и социальной защиты Российской Федерации от 12 декабря 2016 г. № 727н (зарегистрирован Министерством юстиции Российской Федерации 13 января 2017 г., регистрационный № 45230)

Разработчики:	К.э.н. А.А. Шестемиров
Ответственный рецензент:	Назарова Н.А., к.э.н., доцент, заместитель руководителя департамента налогов и налогового администрирования Финансового университета при Правительстве Российской Федерации
	(Ф.И.О., уч. степень, уч. звание, должность)

Рабочая программа дисциплины рассмотрена и одобрена на заседании кафедры инновационного менеджмента и предпринимательства 15.09.2023г., протокол №2

Заведующий кафедрой _____/_____/к.э.н. А.А. Шестемиров/

(подпись)

Согласовано от Библиотеки _____/О.Е. Степкина/

(подпись)

Раздел 1. Цели и задачи освоения дисциплины

Цель курса «Информационная безопасность» состоит в освоение обучающимися основных принципов, моделей и методов защиты информации; овладение методами организационного и правового обеспечения безопасности информационных систем и данных; приобретение навыков и основных приемов защиты информации от утечки и несанкционированного доступа, антивирусной борьбы; применение криптографических методов защиты.

Задачи дисциплины:

- изучить характерные свойства защищаемой информации, основные информационные угрозы, существующие направления защиты;
- получить теоретические знания в области защиты информации;
- ознакомиться с требованиями российских и международных стандартов в области информационной безопасности;
- научиться применять современные программно-аппаратные средства защиты на практике.

Раздел 2. Планируемые результаты обучения по дисциплине, соотнесенные с планируемыми результатами освоения образовательной программы

Категория (группа) компетенций	**Код компетенции**	**Формулировка компетенции**	**Индикаторы достижения компетенции** (для планирования результатов обучения по элементам образовательной программы и соответствующих оценочных средств)
Универсальные компетенции			
Гражданская позиция	УК-10	Способен формировать нетерпимое отношение к коррупционному поведению	ИУК-10.1 Знать признаки коррупционного поведения ИУК-10.2 Уметь проявлять нетерпимое отношение к коррупционному поведению на основе правовых норм и методов борьбы с коррупцией ИУК-10.3 Владеть способами осуществления профессиональную деятельность, основываясь на правовых нормах, в том числе антикоррупционном законодательстве
Общепрофессиональные компетенции			
Общепрофессиональная	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-3.1 Обладает знаниями в области программирования, технологий создания и эксплуатации программных продуктов и программных комплексов ОПК-3.2 Умеет решать стандартные задачи профессиональной деятельности в области программирования, разработки и эксплуатации программных продуктов и программных комплексов ОПК-3.3 Умеет решать стандартные задачи профессиональной деятельности с применением информационных технологий и требований информационной безопасности

Раздел 3. Место дисциплины в структуре образовательной программы

Дисциплина «Информационная безопасность» изучается в шестом семестре, относится к Б1.О.1 Обязательной части учебного плана Блока 1 «Дисциплины (модули)».

Общая трудоемкость дисциплины составляет 3 з.е.

Знания, умения, навыки, опыт практический деятельности, приобретенные при освоении настоящей дисциплины, необходимы для успешного освоения следующих дисциплин: «Проектирование систем управления взаимоотношениями с клиентами», «Компьютерные экспертные системы».

Раздел 4. Объем (трудоемкость) дисциплины

(общая, по видам учебной работы, видам промежуточной аттестации)

Трудоемкость дисциплины и виды учебной работы
(очная форма обучения)

З.е.	Всего часов	Контактная работа				Часы СР на подготовку кур.раб.	Иная СР	Контроль
		Занятия лекционного типа	Занятия семинарского типа		Контактная работа по курсовой работе			
			Лабораторные	Практические/ Семинарские				
6 семестр								
3	108	24	32	-	-	-	50	2 зачет
Всего по дисциплине								
3	108	24	32	-	-	-	50	2

СТРУКТУРА И СОДЕРЖАНИЕ ДИСЦИПЛИНЫ

№ п/п	Наименование разделов и тем дисциплины	Содержание темы
Раздел №1 «Законодательный, процедурный и административный уровни информационной безопасности»		
1	Тема 1.1 Введение в информационную безопасность	Изучаемые вопросы: 1. Понятие информационной безопасности. 2. Основные составляющие информационной безопасности: доступность, целостность и конфиденциальность. 3. Угрозы информационной безопасности. 4. Задачи системы информационной безопасности. 5. Меры противодействия угрозам безопасности. 6. Основные принципы построения систем защиты АИС. Вопросы для самостоятельного изучения: 1. Информационная безопасность на уровне государства. Концепция безопасности РФ. 2. Важность проблемы информационной безопасности. Примеры нарушений информационной безопасности.
2	Тема 1.2 Законодательный уровень информационной безопасности	Изучаемые вопросы: 1. Понятие и важность законодательного уровня информационной безопасности. 2. Обзор российского законодательства в области информационной безопасности. Правовые акты общего назначения, затрагивающие вопросы информационной безопасности. 3. Закон `Об информации, информационных технологиях и о защите информации`. 4. Закон `Об электронной подписи`. 5. Закон `О персональных данных`. 6. Защита авторского права на программные продукты. Вопросы для самостоятельного изучения: 1. Обзор международного законодательства в области информационной безопасности. 2. Федеральный закон `О государственной тайне`.
3	Тема 1.3 Стандарты и спецификации в области информационной безопасности	Изучаемые вопросы: 1. Оценочные стандарты и технические спецификации. 2. Оценочный стандарт ГОСТ Р ИСО/МЭК 15408 `Общие критерии оценки безопасности информационных технологий`. Введение и общая модель. Функциональные компоненты безопасности. Компоненты доверия к безопасности. 3. Сопутствующие документы. Управленческие стандарты информационной безопасности. ГОСТ Р ИСО/МЭК 17799 `Информационные технологии. Практические правила управления

№ п/п	Наименование разделов и тем дисциплины	Содержание темы
		информационной безопасностью`. ГОСТ Р ИСО/МЭК 27001 `Информационные технологии. Методы безопасности. Система управления безопасностью информации. Требования`. Вопросы для самостоятельного изучения: 1. Руководящие документы Гостехкомиссии России.
4	Тема 1.4 Административный уровень информационной безопасности	Изучаемые вопросы: 1. Основные понятия. 2. Политика безопасности. 3. Программа безопасности. 4. Синхронизация программы безопасности с жизненным циклом систем Вопросы для самостоятельного изучения: 1. Примеры типовых политик безопасности организации.
5	Тема 1.5 Процедурный уровень информационной безопасности	Изучаемые вопросы: 1. Основные классы мер процедурного уровня. 2. Управление персоналом. 3. Физическая защита. 4. Поддержка работоспособности 5. Реагирование на нарушение режима безопасности. 6. Планирование восстановительных работ. Вопросы для самостоятельного изучения: 1. План восстановительных работ.
Раздел №2 «Программно-технический уровень информационной безопасности»		
6	Тема 2.1 Идентификация и аутентификация	Изучаемые вопросы: 1. Определение идентификации и аутентификации. 2. Парольная аутентификация. Требования к паролям. 3. Одноразовые пароли. 4. Сервер аутентификации Kerberos. 5. Идентификация/аутентификация с помощью биометрических данных. Вопросы для самостоятельного изучения: 1. Алгоритмы создания одноразовых паролей. 2. Социальный инжиниринг.
7	Тема 2.2 Управление доступом. Протоколирование и аудит	Изучаемые вопросы: 1. Понятие управления доступом. 2. Модели безопасности: модель дискреционного доступа; модель Белла-ЛаПадулы; ролевая модель управления доступом. 3. Понятие протоколирования и аудита. 4. Активный аудит. Вопросы для самостоятельного изучения: 1. Системы разграничения доступа. 2. Функциональные компоненты архитектуры.
8	Тема 2.3 Криптографические методы защиты	Изучаемые вопросы: 1. Введение в криптографию. Основные термины и понятия криптографии. Типы крипто-графических систем. 2. Шифры подстановки и перестановки. 3. Блочные шифры. Сеть Фейштеля. 4. Симметричные алгоритмы шифрования. Алгоритмы DES, ГОСТ 34.12-2015, AES. 5. Асимметричные алгоритмы шифрования. Алгоритм RSA. Вопросы для самостоятельного изучения: 1. Режимы шифрования блочных шифров 2. Потоковые шифры 3. Обмен ключами Диффи-Хелмана. 4. Шифросистема Эль-Гамаля. 5. Стандарт ГОСТ Р 34.10-2012.
9	Тема 2.4 Контроль целост-	Изучаемые вопросы:

№ п/п	Наименование разделов и тем дисциплины	Содержание темы
	ности	1. Определение функции хеширования. Требования к хеш-фукнциям. Функции Хеширова-ния. 2. Электронная цифровая подпись. Цифровые сертификаты. Вопросы для самостоятельного изучения: 1. Деятельность удостоверяющих центров. 2. Функция хеширования MD5.
10	Тема 2.5 Экранирование. Тунелирование	Изучаемые вопросы: 1. Понятие экранирования. Межсетевые экраны. Классификация межсетевых экранов. Виды межсетевых экранов. 2. Понятие тунелирования. Виртуальные частные сети. Вопросы для самостоятельного изучения: 1. VPN IPsec, PPTP. 2. Разработка конфигурации межсетевого экрана.
11	Тема 2.6 Анализ защищенности	Изучаемые вопросы: 1. Понятие анализа защищенности. 2. Сетевые сканеры. 3. Антивирусная защита. Классификация вирусов. Признаки присутствия на компьютере вредоносных программ. 4. Методы защиты от вредоносных программ. Основы работы антивирусных программ. Вопросы для самостоятельного изучения: 1. Антивирусная защита компьютерной сети.

Перечень разделов (модулей), тем дисциплины и распределение учебного времени по разделам/темам дисциплины, видам учебных занятий (в т.ч. контактной работы), видам текущего контроля

очная форма обучения

Разделы / Темы	Контактная работа				Часы СР на подготовку кур. р.	Иная СР	Контроль	Всего часов
	Занятия лекционного типа	Занятия семинарского типа		Контактная работа по кур.р				
		Лаб. р	Прак. /сем.					
6 семестр								
Раздел №1 «Законодательный, процедурный и административный уровни информационной безопасности»	**12**	**12**				**24**		**48**
Тема 1.1 Введение в информационную безопасность	2					2		4
Тема 1.2 Законодательный уровень информационной безопасности	4					4		8
Тема 1.3 Стандарты и спецификации в области информационной безопасности	2	4				6		12
Тема 1.4 Административный уровень информационной безопасности	2	4				6		12
Тема 1.5 Процедурный уровень информационной безопасности	2	4				6		12
Раздел №2 «Программно-технический уровень информа-	**12**	**20**				**26**		**58**

Разделы / Темы	Контактная работа				Часы СР на подготовку кур. р.	Иная СР	Контроль	Всего часов
	Занятия лекционного типа	Занятия семинарского типа		Контактная работа по кур.р				
		Лаб. р	Прак. /сем.					
ционной безопасности»								
Тема 2.1 Идентификация и аутентификация	2					2		4
Тема 2.2 Управление доступом. Протоколирование и аудит	2	4				5		11
Тема 2.3: Криптографические методы защиты	2	4				5		11
Тема 2.4 Контроль целостности	2	4				5		11
Тема 2.5 Экранирование. Тунелирование	2	4				5		11
Тема 2.6 Анализ защищенности	2	4				4		10
Зачет							2	2
Итого за 6 семестр	**24**	**32**				**50**	**2**	**108**

ЗАНЯТИЯ СЕМИНАРСКОГО ТИПА
для очной формы обучения

Семинарские занятия

Общие рекомендации по подготовке к семинарским занятиям. При подготовке к работе во время проведения 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 занятия. Работа во время проведения занятия семинарского типа включает несколько моментов: а) консультирование обучающихся преподавателями с целью предоставления исчерпывающей информации, необходимой для самостоятельного выполнения предложенных преподавателем задач, б) самостоятельное выполнение заданий согласно обозначенной учебной программой тематики.

6 семестр

Раздел №1 «Законодательный, процедурный и административный уровни информационной безопасности»

Лабораторная работа 1. Обзора российского законодательства в области информационной безопасности (4 ч.).

Литература:

Основная

Галатенко, В. А. Основы информационной безопасности : учебное пособие / В. А. Галатенко. - 3-е изд. - Москва : Интернет-Университет Информационных Технологий (ИНТУИТ), Ай Пи Ар Медиа, 2020. - 266 с. - ISBN 978-5-4497-0675-1. - Текст : электронный // Цифровой образовательный ресурс IPR SMART : [сайт]. - URL: https://www.IPRsmart hop.ru/97562.html

Дополнительная

Нестеров С.А., Основы информационной безопасности : учебное пособие / Нестеров С.А.. — Санкт-Петербург : Санкт-Петербургский политехнический университет Петра Великого, 2014. — 322 с. — ISBN 978-5-7422-4331-1. — Текст : электронный // Цифровой образовательный ресурс IPR SMART : [сайт]. — URL: https://www.IPRsmart hop.ru/43960.html

Лабораторная работа 2. Разработка политики безопасности организации (4 ч.).

Литература:

Основная

Галатенко, В. А. Основы информационной безопасности : учебное пособие / В. А. Галатенко. - 3-е изд. - Москва : Интернет-Университет Информационных Технологий (ИНТУИТ), Ай Пи Ар Медиа, 2020. - 266 с. - ISBN 978-5-4497-0675-1. - Текст : электронный // Цифровой образовательный ресурс IPR SMART : [сайт]. - URL: https://www.IPRsmart hop.ru/97562.html

Дополнительная

Нестеров С.А., Основы информационной безопасности : учебное пособие / Нестеров С.А.. — Санкт-Петербург : Санкт-Петербургский политехнический университет Петра Великого, 2014. — 322 с. — ISBN 978-5-7422-4331-1. — Текст : электронный // Цифровой образовательный ресурс IPR SMART : [сайт]. — URL: https://www.IPRsmart hop.ru/43960.html

Лабораторная работа 3. Анализ рисков информационной безопасности организации (4 ч.).

Литература:

Основная

Галатенко, В. А. Основы информационной безопасности : учебное пособие / В. А. Галатенко. - 3-е изд. - Москва : Интернет-Университет Информационных Технологий (ИНТУИТ), Ай Пи Ар Медиа, 2020. - 266 с. - ISBN 978-5-4497-0675-1. - Текст : электронный // Цифровой образовательный ресурс IPR SMART : [сайт]. - URL: https://www.IPRsmart hop.ru/97562.html

Дополнительная

Нестеров С.А., Основы информационной безопасности : учебное пособие / Нестеров С.А.. — Санкт-Петербург : Санкт-Петербургский политехнический университет Петра Великого, 2014. — 322 с. — ISBN 978-5-7422-4331-1. — Текст : электронный // Цифровой образовательный ресурс IPR SMART : [сайт]. — URL: https://www.IPRsmart hop.ru/43960.html

Раздел №2 «Программно-технический уровень информационной безопасности»

Лабораторная работа 4. Защита информации в компьютерной системе от случайных угроз. Создание и управление учетными записями пользователей (4 ч.).

Литература:

Основная

Галатенко, В. А. Основы информационной безопасности : учебное пособие / В. А. Галатенко. - 3-е изд. - Москва : Интернет-Университет Информационных Технологий (ИНТУИТ), Ай Пи Ар Медиа, 2020. - 266 с. - ISBN 978-5-4497-0675-1. - Текст : электронный // Цифровой образовательный ресурс IPR SMART : [сайт]. - URL: https://www.IPRsmart hop.ru/97562.html

Дополнительная

Нестеров С.А., Основы информационной безопасности : учебное пособие / Нестеров С.А.. — Санкт-Петербург : Санкт-Петербургский политехнический университет Петра Великого, 2014. — 322 с. — ISBN 978-5-7422-4331-1. — Текст : электронный // Цифровой образовательный ресурс IPR SMART : [сайт]. — URL: https://www.IPRsmart hop.ru/43960.html

Лабораторная работа 5. Обеспечение безопасности ресурсов с помощью разрешений файловой системы NTFS. Аудит ресурсов и событий системы защиты (4 ч.).

Литература:

Основная

Галатенко, В. А. Основы информационной безопасности : учебное пособие / В. А. Галатенко. - 3-е изд. - Москва : Интернет-Университет Информационных Технологий (ИНТУИТ), Ай Пи Ар Медиа, 2020. - 266 с. - ISBN 978-5-4497-0675-1. - Текст : электронный // Цифровой образовательный ресурс IPR SMART : [сайт]. - URL: https://www.IPRsmart hop.ru/97562.html

Дополнительная

Нестеров С.А., Основы информационной безопасности : учебное пособие / Нестеров С.А.. — Санкт-Петербург : Санкт-Петербургский политехнический университет Петра Великого, 2014. — 322 с. — ISBN 978-5-7422-4331-1. — Текст : электронный // Цифровой образовательный ресурс IPR SMART : [сайт]. — URL: https://www.IPRsmart hop.ru/43960.html

Лабораторная работа 6. Настройка системных параметров безопасности (4 ч.).

Литература:

Основная

Галатенко, В. А. Основы информационной безопасности : учебное пособие / В. А. Галатенко. - 3-е изд. - Москва : Интернет-Университет Информационных Технологий (ИНТУИТ), Ай Пи Ар Медиа, 2020. - 266 с. - ISBN 978-5-4497-0675-1. - Текст : электронный // Цифровой образовательный ресурс IPR SMART : [сайт]. - URL: https://www.IPRsmart hop.ru/97562.html

Дополнительная

Нестеров С.А., Основы информационной безопасности : учебное пособие / Нестеров С.А.. — Санкт-Петербург : Санкт-Петербургский политехнический университет Петра Великого, 2014. — 322 с. — ISBN 978-5-7422-4331-1. — Текст : электронный // Цифровой образовательный ресурс IPR SMART : [сайт]. — URL: https://www.IPRsmart hop.ru/43960.html

Лабораторная работа 7. Настройка параметров безопасности подключения к Интернет(4 ч.).

Литература:

Основная

Галатенко, В. А. Основы информационной безопасности : учебное пособие / В. А. Галатенко. - 3-е изд. - Москва : Интернет-Университет Информационных Технологий (ИНТУИТ), Ай Пи Ар Медиа, 2020. - 266 с. - ISBN 978-5-4497-0675-1. - Текст : электронный // Цифровой образовательный ресурс IPR SMART : [сайт]. - URL: https://www.IPRsmart hop.ru/97562.html

Дополнительная

Нестеров С.А., Основы информационной безопасности : учебное пособие / Нестеров С.А.. — Санкт-Петербург : Санкт-Петербургский политехнический университет Петра Великого, 2014. — 322 с. — ISBN 978-5-7422-4331-1. — Текст : электронный // Цифровой образовательный ресурс IPR SMART : [сайт]. — URL: https://www.IPRsmart hop.ru/43960.html

Лабораторная работа 8. Разработка алгоритмов криптографической защиты(4 ч.).

Литература:

Основная

Галатенко, В. А. Основы информационной безопасности : учебное пособие / В. А. Галатенко. - 3-е изд. - Москва : Интернет-Университет Информационных Технологий (ИНТУИТ), Ай Пи Ар Медиа, 2020. - 266 с. - ISBN 978-5-4497-0675-1. - Текст : электронный // Цифровой образовательный ресурс IPR SMART : [сайт]. - URL: https://www.IPRsmart hop.ru/97562.html

Дополнительная

Нестеров С.А., Основы информационной безопасности : учебное пособие / Нестеров С.А.. — Санкт-Петербург : Санкт-Петербургский политехнический университет Петра Великого, 2014. — 322 с. — ISBN 978-5-7422-4331-1. — Текст : электронный // Цифровой образовательный ресурс IPR SMART : [сайт]. — URL: https://www.IPRsmart hop.ru/43960.html

РАЗДЕЛ 5. ОБРАЗОВАТЕЛЬНЫЕ ТЕХНОЛОГИИ

Интерактивные образовательные технологии, используемые на аудиторных лабораторных занятиях

Очная форма обучения

Наименование разделов, тем	Используемые образовательные технологии	Часы
Раздел №1 «Законодательный, процедурный и административный уровни информационной безопасности» Тема 1.1 Введение в информационную безопасность Тема 1.2 Законодательный уровень информационной безопасности Тема 1.3 Стандарты и спецификации в области информационной безопасности Тема 1.4 Административный уровень информационной безопасности Тема 1.5 Процедурный уровень информационной безопасности	Обсуждение решений профессионально-ориентированных заданий и задач; обсуждение и анализ решения кейсов	**2**
Раздел №2 «Программно-технический уровень информационной безопасности» Тема 2.1 Идентификация и аутентификация Тема 2.2 Управление доступом. Протоколирование и аудит Тема 2.3: Криптографические методы защиты Тема 2.4 Контроль целостности Тема 2.5 Экранирование. Тунелирование Тема 2.6 Анализ защищенности	Обсуждение решений профессионально-ориентированных заданий и задач; обсуждение и анализ решения кейсов	**2**

РАЗДЕЛ 6. УЧЕБНО-МЕТОДИЧЕСКОЕ ОБЕСПЕЧЕНИЕ САМОСТОЯТЕЛЬНОЙ РАБОТЫ ОБУЧАЮЩИХСЯ ПО ДИСЦИПЛИНЕ

Самостоятельная работа

Наименование разделов/тем	Вопросы, выносимые на самостоятельное изучение
Раздел №1 «Законодательный, процедурный и административный уровни информационной безопасности» Тема 1.1 Введение в информационную безопасность Тема 1.2 Законодательный уровень информационной безопасности Тема 1.3 Стандарты и спецификации в области информационной безопасности Тема 1.4 Административный уровень информационной безопасности Тема 1.5 Процедурный уровень информационной безопасности	1. Информационная безопасность на уровне государства. Концепция безопасности РФ. 2. Важность проблемы информационной безопасности. Примеры нарушений информационной безопасности. 3. Обзор международного законодательства в области информационной безопасности. 4. Федеральный закон `О государственной тайне`. 5. Руководящие документы Гостехкомиссии России. 6. Примеры типовых политик безопасности организации. 7. План восстановительных работ.
Раздел №2 «Программно-технический уровень информационной безопасности» Тема 2.1 Идентификация и аутентификация Тема 2.2 Управление доступом. Протоколирование и аудит Тема 2.3: Криптографические методы защиты Тема 2.4 Контроль целостности Тема 2.5 Экранирование. Тунелирование Тема 2.6 Анализ защищенности	1. Алгоритмы создания одноразовых паролей. 2. Социальный инжиниринг. 3. Системы разграничения доступа. 4. Функциональные компоненты архитектуры. 5. Режимы шифрования блочных шифров 6. Потоковые шифры 7. Обмен ключами Диффи-Хелмана. 8. Шифросистема Эль-Гамаля. 9. Стандарт ГОСТ Р 34.10-2012. 10. Деятельность удостоверяющих центров. 11. Функция хеширования MD5. 12. VPN IPsec, PPTP. 13. Разработка конфигурации межсетевого экрана. 14. Антивирусная защита компьютерной сети.

6.1. Примерные задания для самостоятельной работы

1. (Кейс-задание). Расчет рисков информационной безопасности

Описание ситуации:

Например, информационная система Компании состоит из двух ресурсов: сервера и рабочей станции, которые находятся в одной сетевой группе, т.е. физически связанны между собой.

На сервере хранятся виды информации: бухгалтерский отчет и база кли-ентов Компании.

На рабочей станции расположена база данных наименований товаров Компании с описанием. К серверу локальный доступ имеет группа пользователей (к первой информации – бухгалтерский отчет):

 главный бухгалтер.

К серверу удаленный доступ имеют группы пользователей (ко второй информации – база клиентов Компании):

 бухгалтер (с рабочей станции);

 финансовый директор (через глобальную сеть Интернет).

К рабочей станции локальный доступ имеет группа пользователей (к базе данных наименований товаров Компании с описанием):

 бухгалтер.

По правилам работы модели бухгалтер при удаленном доступе к серверу является группой обычных пользователей, а финансовый директор – группой авторизованных пользователей. Причем, бухгалтер имеет удаленный доступ к серверу через коммутатор.

Задание: Рассчитать риски информационной безопасности на основе мо-дели информационных потоков.

2. (Кейс-задание).
Описание ситуации:
В одной из компаний сотрудник хранил на мобильном компьютере кон-фиденциальные сведения компании без применения средств шифрования. После работы он забрал компьютер домой и забыл его в машине, которую оставил под окнами дома, а ночью машину взломали, и компьютер был украден. Злоумышленники получили доступ к конфиденциальной информации компании и могли продать ее конкурентам. Кроме этого, на компьютере хранилась ценная информация, которая не была зарезервирована на другом носителе.

Задание.
1. Определите возможные причины инцидента и степень ответственности сотрудника.
2. Определите меры, направленные на предотвращение повторных инци-дентов.

3. (Кейс-задание).
Описание ситуации.
В одной из компаний клиентке вместе со счетом на оплату выдали список других клиентов. В списке были указаны фамилии, имена, даты рождения, домашние адреса и паспортные данные.

Задание.
1. Определите возможные причины инцидента и степень ответственности сотрудника.
2. Определите меры, направленные на предотвращение повторных инци-дентов.

4. Выполните следующие практическое задание:
1. Создайте точку восстановления.
2. Создайте 2-х пользователей User-1(администратор компьютера), User-2 (ограниченная запись). Для каждого пользователя потребуйте смену пароля при первом входе в систему.
3. Создайте группу Test и добавьте в нее созданных пользователей.
4. Создайте папку Test в которой разместите три файла text1.txt, text2.txt, text3.txt. Владельцем файла text1.txt сделайте пользователя User-1.
5. Для файла text2.txt настройте следующие права для пользователей и групп:
User-1 – чтение, запись, удаление, чтение разрешений, смена раз-решений
User-2 – чтение и выполнение
Группа Test – изменение и запись

5. Выполните следующее практическое задание:
1. Создайте резервную копию системной информации.
2. Создайте 2-х пользователей User-1(администратор компьютера), User-2 (ограниченная запись). Для каждого пользователя потребуйте смену пароля при первом входе в систему.
3. Задайте системные параметры безопасности. Учетная запись пользователя блокируется после 3 неверных попыток ввода пароля.
4. Настройте аудит безопасности. Просмотрите журнал событий для пользователя User-2.
5. Создайте и зашифруйте файла text.txt

РАЗДЕЛ 7. ОЦЕНОЧНЫЕ И МЕТОДИЧЕСКИЕ МАТЕРИАЛЫ ПО ОБРАЗОВАТЕЛЬНОЙ ПРОГРАММЕ (ФОНД ОЦЕНОЧНЫХ СРЕДСТВ) ДЛЯ ПРОВЕДЕНИЯ ТЕКУЩЕГО КОНТРОЛЯ УСПЕВАЕМОСТИ И ПРОМЕЖУТОЧНОЙ АТТЕСТАЦИИ

7.1. Форма промежуточной аттестации обучающегося по учебной дисциплине.

Контрольным мероприятием промежуточной аттестации обучающихся по учебной дисциплине «Информационная безопасность» в 6 семестре является зачет**,** который проводится в форме теста.

Таблица 7.1

ПЛАНИРУЕМЫЕ РЕЗУЛЬТАТЫ ОБУЧЕНИЯ ПО ДИСЦИПЛИНЕ, СООТНЕСЕННЫЕ С ПЛАНИРУЕМЫМИ РЕЗУЛЬТАТАМИ ОСВОЕНИЯ ОБРАЗОВАТЕЛЬНОЙ ПРОГРАММЫ В СООТНОШЕНИИ С ОЦЕНОЧНЫМИ СРЕДСТВАМИ

Планируемые результаты, характеризующие этапы формирования компетенции	**Содержание учебного материала**	**Примеры контрольных вопросов и заданий для оценки знаний, умений, владений**	**Методы/ средства контроля**
УК-10 Способен формировать нетерпимое отношение к коррупционному поведению			
ИУК-10.1 Знать признаки коррупционного поведения	Раздел №1 «Законодательный, процедурный и административный уровни информационной безопасности» Тема 1.1 Введение в информационную безопасность Тема 1.2 Законодательный уровень информационной безопасности Тема 1.3 Стандарты и спецификации в области информационной безопасности Тема 1.4 Административный уровень информационной безопасности Тема 1.5 Процедурный уровень информационной безопасности Раздел №2 «Программно-технический уровень информационной безопасности» Тема 2.1 Идентификация и аутентификация Тема 2.2 Управление доступом. Протоколирование и аудит Тема 2.3: Криптографические методы защиты Тема 2.4 Контроль целостности Тема 2.5 Экранирование. Тунелирование Тема 2.6 Анализ	Основные понятия информационной безопасности. Классификация угроз. Классификация средств защиты информации. Законодательная основа информационной безопасности	Устный контроль/ опрос на семинарских занятиях, зачете, экзамене; анализ докладов на семинарских занятиях; анализ защиты рефератов; анализ защиты проектов; применение теоретических знаний при анализе (разборе) конкретных практико-ориентированных ситуаций и профессионально-прикладных задач, анализ использования теоретических знаний в процессе решения кейсов, в ходе деловых игр; письменный контроль, анализ содержания эссе; тестирование (выполнение тестовых заданий)
ИУК-10.2 Уметь проявлять нетерпимое отношение к коррупционному поведению на основе правовых норм и методов борьбы с коррупцией	Раздел №1 «Законодательный, процедурный и административный уровни информационной безопасности» Тема 1.1 Введение в информационную безопасность Тема 1.2 Законодательный уровень информационной безопасности Тема 1.3 Стандарты и спецификации в области информационной безопасности Тема 1.4 Административный уровень информационной безопасности Тема 1.5 Процедурный уровень информационной безопасности Раздел №2 «Программно-технический уровень информационной безопасности» Тема 2.1 Идентификация и аутентификация Тема 2.2 Управление доступом. Протоколирование и аудит Тема 2.3: Криптографические методы защиты Тема 2.4 Контроль целостности Тема 2.5 Экранирование. Тунелирование Тема 2.6 Анализ	Методы и средства организационно-правовой защиты информации. Методы и средства инженерно-технической защиты.	Анализ проявленных умений при решении кейсов, в ходе деловых игр; письменный контроль, анализ качества решений профессиональных задач в контрольных работах; анализ содержания профессионально-ориентированных эссе; тестирование (выполнение тестовых заданий); анализ защит профессионально-ориентированных проектов; опрос на семинарских занятиях, зачете, анализ докладов на семинарских занятиях; анализ защиты рефератов; анализ решения конкретных практико-ориентированных

			ситуаций и профессионально-прикладных задач, анализ выполнения контрольных работ
ИУК-10.3 Владеть способами осуществления профессиональную деятельность, основываясь на правовых нормах, в том числе антикоррупционном законодательстве	Раздел №1 «Законодательный, процедурный и административный уровни информационной безопасности» Тема 1.1 Введение в информационную безопасность Тема 1.2 Законодательный уровень информационной безопасности Тема 1.3 Стандарты и спецификации в области информационной безопасности Тема 1.4 Административный уровень информационной безопасности Тема 1.5 Процедурный уровень информационной безопасности Раздел №2 «Программно-технический уровень информационной безопасности» Тема 2.1 Идентификация и аутентификация Тема 2.2 Управление доступом. Протоколирование и аудит Тема 2.3: Криптографические методы защиты Тема 2.4 Контроль целостности Тема 2.5 Экранирование. Тунелирование Тема 2.6 Анализ	Организационно-правовые и программные и программно-аппаратные методы и средства обеспечения информационной безопасности	Анализ проявленных навыков при решении кейсов, в ходе деловых игр; письменный контроль, анализ качества решений профессиональных задач в контрольных работах; анализ содержания профессионально-ориентированных эссе; тестирование (выполнение тестовых заданий); анализ защит профессионально-ориентированных проектов; опрос на семинарских занятиях, зачете, экзамене; анализ докладов на семинарских занятиях; анализ защиты рефератов; анализ решения конкретных практико-ориентированных ситуаций и профессионально-прикладных задач, анализ выполнения контрольных работ
ОПК-3 Способен решать стандартные задачи профессиональной деятельности на основе информационной и библиографической культуры с применением ин-формационно-коммуникационных технологий и с учетом основных требований информационной безопасности			
ИОПК-3.1. Знать в области программирования, технологии создания и эксплуатации программных продуктов и программных комплексов	Раздел №1 «Законодательный, процедурный и административный уровни информационной безопасности» Тема 1.1 Введение в информационную безопасность Тема 1.2 Законодательный уровень информационной безопасности Тема 1.3 Стандарты и спецификации в области информационной безопасности Тема 1.4 Административный уровень информационной безопасности Тема 1.5 Процедурный уровень информационной безопасности Раздел №2 «Программно-технический уровень информационной безопасности» Тема 2.1 Идентификация и аутентификация Тема 2.2 Управление доступом. Протоколирование и аудит Тема 2.3: Криптографические методы защиты Тема 2.4 Контроль целостности Тема 2.5 Экранирование. Тунелиро-	Введение в основы современных шифров с симметричным ключом. Модульная арифметика. Сравнения и матрицы. Традиционные шифры с симметричным ключом. Алгебраические структуры. Поля. Усовершенствованный стандарт шифрования (AES — Advanced Encryption Standard). Простые числа. Квадратичное сравнение. Криптографическая система RSA. Криптосистемы. Простые криптосистемы. Шифрование методом замены (подстановки). Одноалфавитная подстановка. Многоалфавитная одноконтурная обыкновенная подстановка. Таблицы Вижинера. Многоалфавитная одноконтурная монофоническая подстановка. Многоалфавитная многоконтурная подстановка.	Устный контроль/ опрос на семинарских занятиях, зачете, экзамене; анализ докладов на семинарских занятиях; анализ защиты рефератов; анализ защиты проектов; применение теоретических знаний при анализе (разборе) конкретных практико-ориентированных ситуаций и профессионально-прикладных задач, анализ использования теоретических знаний в процессе решения кейсов, в ходе деловых игр; письменный контроль, анализ со-

	вание Тема 2.6 Анализ	Шифрование методом перестановки. Простая перестановка. Перестановка, усложненная по таблице. Перестанов- ка, усложненная по маршрутам. Шифрование методом гаммирования. Шифрование с помощью аналитических преобразований. Комбинированные методы шифрования. Стандарты шифрования. Стандарт шифрования данных Data Encryption Standard. Режимы работы алгоритма DES. Алгоритм шифрования данных IDEA. Общая схема алгоритма IDEA	держания эссе; тестирование (выполнение тестовых заданий)
ИОПК-3.2. Умеет решать стандартные задачи профессиональной деятельности в области программирования, разработки и эксплуатации программных продуктов и программных комплексов	Раздел №1 «Законодательный, процедурный и административный уровни информационной безопасности» Тема 1.1 Введение в информационную безопасность Тема 1.2 Законодательный уровень информационной безопасности Тема 1.3 Стандарты и спецификации в области информационной безопасности Тема 1.4 Административный уровень информационной безопасности Тема 1.5 Процедурный уровень информационной безопасности Раздел №2 «Программно-технический уровень информационной безопасности» Тема 2.1 Идентификация и аутентификация Тема 2.2 Управление доступом. Протоколирование и аудит Тема 2.3: Криптографические методы защиты Тема 2.4 Контроль целостности Тема 2.5 Экранирование. Тунелирование Тема 2.6 Анализ	Общие понятия антивирусной защиты. Уязвимости. Классификация вредоносных программ. Признаки присутствия на компьютере вредоносных программ. Методы защиты от вредоносных программ. Основы работы антивирусных программ: Сигнатурный и эвристический анализ. Тестирование работы антивируса. Классификация антивирусов. Режимы работы антивирусов. Антивирусные комплексы	Анализ проявленных умений при решении кейсов, в ходе деловых игр; письменный контроль, анализ качества решений профессиональных задач в контрольных работах; анализ содержания профессионально-ориентированных эссе; тестирование (выполнение тестовых заданий); анализ защит профессионально-ориентированных проектов; опрос на семинарских занятиях, зачете, анализ докладов на семинарских занятиях; анализ защиты рефератов; анализ решения конкретных практико-ориентированных ситуаций и профессионально-прикладных задач, анализ выполнения контрольных работ
ИОПК-3.3. Владеть решением стандартных задач в профессиональной деятельности с применением информационных технологий и требований информационной безопасности	Раздел №1 «Законодательный, процедурный и административный уровни информационной безопасности» Тема 1.1 Введение в информационную безопасность Тема 1.2 Законодательный уровень информационной безопасности Тема 1.3 Стандарты и спецификации в области информационной безопасности Тема 1.4 Административный уровень информационной безопасности Тема 1.5 Процедурный уровень информационной безопасности Раздел №2 «Программно-технический уровень информацион-	Защита информации в локальных сетях Уровни антивирусной защиты. Уровень защиты рабочих станций и сетевых серверов. Уровень защиты почты. Уровень защиты шлюзов. Централизованное управление антивирусной защитой. Логическая сеть. Схема сбора статистики в системе антивирусной защиты. Управление ключами шифрования и без-	Анализ проявленных навыков при решении кейсов, в ходе деловых игр; письменный контроль, анализ качества решений профессиональных задач в контрольных работах; анализ содержания профессионально-ориентированных эссе; тестирование (выполнение тестовых заданий); анализ защит про-

	ной безопасности» Тема 2.1 Идентификация и аутентификация Тема 2.2 Управление доступом. Протоколирование и аудит Тема 2.3: Криптографические методы защиты Тема 2.4 Контроль целостности Тема 2.5 Экранирование. Тунелирование Тема 2.6 Анализ	опасность сети. Целостность сообщения и установление подлинности сообщения. Криптографические хэш-функции. Цифровая подпись. Установление подлинности объекта. Управление ключами. Безопасность на прикладном уровне: PGP и S/MIME. Безопасность на транспортном уровне: SSL и TLS. Безопасность на сетевом уровне: IP SEC. Брандмауэры. Определение типов брандмауэров. Разработка конфигурации межсетевого экрана. Построение набора правил межсетевого экрана. Система обнаружения вторжений (IDS). Узловые IDS. Анализаторы журналов. Датчики признаков. Анализаторы системных вызовов. Анализаторы поведения приложений. Контроллеры целостности файлов. Сетевые IDS. Установка IDS. Определение целей применения IDS. Управление IDS	фессионально-ориентированных проектов; опрос на семинарских занятиях, зачете, экзамене; анализ докладов на семинарских занятиях; анализ защиты рефератов; анализ решения конкретных практико-ориентированных ситуаций и профессионально-прикладных задач, анализ выполнения контрольных работ

7.2. Примеры тестовых вопросов для подготовки к промежуточной аттестации (зачет)

1. В Интернете размещен информационный портал. Стало известно, что при попытке зайти на него выдается сообщение такого плана:
"503 Service Temporarily Unavailable.
The server is temporarily unable to service your request due to maintenance downtime or capacity problems.
Please try again later."
Какое из перечисленных свойств защищенной информации было нарушено?

- Наблюдаемость
- Целостность
- Конфиденциальность
- Доступность
- Массовость

2. Что из перечисленного не является целью проведения аудита безопасности?

- Выработка рекомендаций по внедрению новых и повышению эффективности существующих механизмов безопасности системы
- Локализация "узких мест" в системе защиты системы
- Оценка будущего уровня защищенности системы
- Анализ рисков, связанных с возможностью осуществления угроз безопасности в отношении ресурсов системы
- Оценка соответствия системы существующим стандартам в области информационной безопасности

3. Попытка реализации угрозы информационной безопасности - это... (выберите понятие в

терминах информационной безопасности)
- Нападение
- Атака
- Штурм
- Контратака
- Уязвимость

4. Укажите перечень грифов секретности для носителей сведений, составляющих государственную тайну (согласно законодательству РФ).
- Совершенно секретно
- Для служебного пользования
- Особой важности
- Секретно
- Гос.тайна

5. Каким термином (согласно законодательству РФ) можно назвать защищаемые государством сведения в области его военной, внешнеполитической, экономической, разведывательной, контрразведывательной и оперативно-розыскной деятельности, распространение которых может нанести ущерб безопасности Российской Федерации?
- Военная тайна
- Информация для служебного использования
- Секретная информация
- Государственная тайна
- Конфиденциальная информация

6. Вы получили по электронной почте письмо с вложением "От отдела IT". В тексте письма говорится, что ваш компьютер был заражен вирусом. Поэтому вам необходимо открыть вложение и следовать инструкциям, чтобы избавиться от вируса. Что необходимо сделать? (Выберите все подходящие варианты).
- Откройте вложение, чтобы увидеть его содержание.
- Написать письмо отправителю с просьбой удалить из списка рассылки.
- Следуйте инструкциям, чтобы удалить вирус.
- Связаться с IT-отделом для уточнения информации о полученном письме.
- Удалить сообщение из неизвестного источника.

7. Кто из следующих лиц несет основную ответственность за определение уровня классификации информации?
- Администратор
- Владелец
- Аудитор
- Пользователь
- Менеджер по безопасности

8. Какие технические средства из перечисленных не подлежат сертификации?
- Защищенные информационные системы
- Защищенные технические средства обработки информации
- Средства выявления программных закладок

 Средства криптографической защиты информации
 Нет верного ответа

9. Какая категория является наиболее рискованной для компании с точки зрения вероятного мошенничества и нарушения безопасности ?
 Сотрудники
 Хакеры
 Атакующие
 Посетители
 Контрагенты (лица, работающие по договору)

10. Каким термином (согласно законодательству РФ) называется любая информация, относящаяся к прямо или косвенно определенному или определяемому физическому лицу?
 Персональные данные
 Информация про личность
 Конфиденциальная информация
 Государственная тайна
 Информация с ограниченным доступом

11. Лицо, самостоятельно создавшее информацию либо получившее на основании закона или договора право разрешать или ограничивать доступ к информации?
 Источник информации
 Потребитель информации
 Уничтожитель информации
 Носитель информации
 Обладатель информации

12. Отношения, связанные с обработкой персональных данных, регулируются законом …
 «Об информации, информационных технологиях и о защите информации»
 «О защите информации»
 Федеральным законом «О персональных данных»
 Федеральным законом «О конфиденциальной информации»
 «Об утверждении перечня сведений конфиденциального характера»

13. Наиболее опасным источником угроз информационной безопасности предприятия являются?
 Другие предприятия (конкуренты)
 Сотрудники информационной службы предприятия, имеющие полный доступ к его информационным ресурсам
 Рядовые сотрудники предприятия
 Возможные отказы оборудования, отключения электропитания, нарушения в сети передачи данных
 Хакеры

14. Информация об уголовной ответственности за преступление в сфере компьютерной информации описана в?
 1 главе Уголовного кодекса

 5 главе Уголовного кодекса
 28 главе Уголовного кодекса
 100 главе Уголовного кодекса
 1000 главе Уголовного кодекса

15. Какой фактор наиболее важен для того, чтобы быть уверенным в успешном обеспечении безопасности в компании?
 Поддержка высшего руководства
 Эффективные защитные меры и методы их внедрения
 Актуальные и адекватные политики и процедуры безопасности
 Проведение тренингов по безопасности для всех сотрудников

16. Что из перечисленного не относится к сфере действия федерального закона «Об информации, информационных технологиях и о защите информации» направлен на?
 Осуществление права на поиск, получение, передачу, производство и распространение информации;
 применении информационных технологий;
 обеспечении защиты информации.
 Регулирование требований к работникам служб, работающих с информаций
 Формирование необходимых норм и правил, связанных с защитой детей от информации

17. Когда целесообразно не предпринимать никаких действий в отношении выявленных рисков?
 Никогда. Для обеспечения хорошей безопасности нужно учитывать и снижать все риски
 Когда риски не могут быть приняты во внимание по политическим соображениям
 Когда необходимые защитные меры слишком сложны
 Когда стоимость контрмер превышает ценность актива и потенциальные потери

18. Что из перечисленного не является целью проведения анализа рисков?
 Делегирование полномочий
 Количественная оценка воздействия потенциальных угроз
 Выявление рисков
 Определение баланса между воздействием риска и стоимостью необходимых контрмер

19. Что такое политики безопасности?
 Пошаговые инструкции по выполнению задач безопасности
 Общие руководящие требования по достижению определенного уровня безопасности
 Совокупность документированных руководящих принципов, правил, процедур и практических приёмов инициированные руководством
 Детализированные документы по обработке инцидентов безопасности

20. Основной документ, на основе которого проводится политика информационной безопасности?
 Программа информационной безопасности
 Регламент информационной безопасности
 Политическая информационная безопасность
 Протекторат

21. Информационная безопасность – …

1. комплекс мероприятий направленных на обеспечение защиты информации.
2. защищённость информации и поддерживающей инфраструктуры от случайных или преднамеренных воздействий естественного или искусственного характера, которые могут нанести неприемлемый ущерб субъектам информационных отношений.
3. целенаправленная деятельность организации и ее должностных лиц с использованием разрешённых сил и средств по достижению состояния защищённости информационной среды организации, обеспечивающее её нормальное функционирование и динамичное развитие.
4. комплекс мероприятий направленных на предотвращение несанкционированной модификации информации.

22. Угроза это …

1) потенциальная возможность определенным образом нарушить информационную безопасность
2) возможность использования слабых мест в защите информационной системы
3) существование ошибок и архитектурных просчетов в защищаемой информационной системе
4) успешная атака на информационную систему

23. Злоумышленником называют …

1) нарушителя, намеренного идущего на нарушение из корыстных побуждений
2) лицо, предпринявшее попытку выполнения запрещенных действий
3) лицо, предпринявшее попытку выполнения запрещенных действий по незнанию
4) нарушителя, намеренного идущего на нарушение без корыстных побуждений

24. Какой закон в числе своих принципов содержит гарантии недопущения сбора, хранения, использования и распространения информации о частной жизни лица без его согласия

1) Указ Президента РФ
2) Закон «Об информации, информационных технологиях и о защите информации»
3) Раздел «Преступления в сфере компьютерной информации» Уголовного кодекса РФ
4) Закон «О безопасности»

25. Согласно руководящим документам Гостехкомиссии РФ под несанкционированным доступом (НСД) понимается

1) вход в систему без согласования с руководством организации
2) доступ к информации, превышающий установленный уровень доступа
3) доступ к информации, нарушающий установленные правила разграничения доступа
4) доступ к информации с использованием средств действующих в обход средств защиты

26. Какой части нет в стандарте «Общие критерии»

1) Введение и общая модель
2) Функциональные требования безопасности
3) Требования доверия к безопасности
4) Классы безопасности

27. Политика безопасности – это

1) совокупность документированных решений, принимаемых руководством организации и направленных на защиту информации и ассоциированных с ней ресурсов
2) определенная нормативно-правовыми документами система взглядов государства на проблемы информационной безопасности
3) правила выбора средств защиты от угроз информационной безопасности
4) полный набор архитектурных правил безопасности

28. Основой программы безопасности организации является
1) решения правительства РФ
2) политика безопасности организации
3) отчет начальника службы информационной безопасности
4) указание надзирающего органа

29. По отношению к выявленным рискам возможны следующие действия
1) ликвидация риска
2) уменьшение риска
3) принятие риска
4) все выше перечисленное

30. Идентификация позволяет …
1) убедится в том, что субъект действительно тот за кого себя выдает
2) выявить нарушителя
3) субъекту назвать себя
4) регистрировать действия пользователя в системе

31. Под протоколированием понимается
1) ведение протокола выявленных нарушений информационной безопасности
2) накопление информации о событиях, происходящих в информационной системе
3) анализ накопленной в системе информации
4) накопление информации о изменении прав доступа к файлам системы

32. Для реализации каких сервисов безопасности могут быть использованы криптографические методы
1) шифрование
2) контроль целостности
3) управление доступом
4) экранирование

33. В число классов мер процедурного уровня входят:
1) управление персоналом
2) идентификация и аутентификация
3) физическая защита
4) управление доступом

34. Сколько групп символов должен минимально содержать надежный пароль
Ответ: _____

35. В какой модели доступа для каждого объекта существует субъект-владелец, который сам определяет тех, кто имеет доступ к объекту, а также разрешенные операции доступа

1) дискреционной модели доступа
2) модели мандатного доступа
3) ролевой модели доступа
4) модели Белла-ЛаПадулы

36. Центральным для программно-технического уровня является понятие
Ответ: _____

37. Установите соответствие описания мер противодействия угрозам безопасности группам мер безопасности

А. Действующие в стране нормативно-правовые акты, регламентирующие правила обращения с информацией, закрепляющие права и обязанности участников информационных отношений в процессе ее обработки и использования, а также устанавливающие ответственность за нарушения этих правил.

Б. Меры организационного характера, регламентирующие процессы функционирования АИС, деятельность персонала, а также порядок взаимодействия пользователей с системой таким образом, чтобы в наибольшей степени затруднить или исключить возможность реализации угроз безопасности.

В. Отдельные мероприятия, выполняемые на протяжении всего жизненного цикла АИС. Ориентированы прежде всего на людей, а не на технические средства.
Варианты ответов:

1) Административная
2) Законодательная
3) Программно-техническая
4) Процедурная

А	Б	В

Ответ:

А	Б	В
2	1	4

7.3. Описание показателей и критериев оценивания сформированности компетенций на различных этапах их формирования; шкалы и процедуры оценивания

7.3.1. Оценивание ответов на вопросы и выполнения заданий для текущей и промежуточной аттестации

При оценке знаний учитывается уровень сформированности компетенций:

1. Уровень усвоения теоретических положений дисциплины, правильность формулировки основных понятий и закономерностей.
2. Уровень знания фактического материала в объеме программы.
3. Логика, структура и грамотность изложения вопроса.
4. Умение связать теорию с практикой.

5. Умение делать обобщения, выводы.

Шкала оценивания на зачете

Оценка	Критерии выставления оценки
Зачтено	Обучающийся должен: - продемонстрировать общее знание изучаемого материала; - показать общее владение понятийным аппаратом дисциплины; - уметь строить ответ в соответствии со структурой излагаемого вопроса; - знать основную рекомендуемую программой учебную литературу.
Не зачтено	Обучающийся демонстрирует: - незнание значительной части программного материала; - не владение понятийным аппаратом дисциплины; - существенные ошибки при изложении учебного материала; - неумение строить ответ в соответствии со структурой излагаемого вопроса; - неумение делать выводы по излагаемому материалу.

7.4. МЕТОДИЧЕСКИЕ МАТЕРИАЛЫ, ОПРЕДЕЛЯЮЩИЕ ПРОЦЕДУРЫ ОЦЕНИВАНИЯ ЗНАНИЙ, УМЕНИЙ, НАВЫКОВ И (ИЛИ) ОПЫТА ДЕЯТЕЛЬНОСТИ, ХАРАКТЕРИЗУЮЩИХ ЭТАПЫ ФОРМИРОВАНИЯ КОМПЕТЕНЦИЙ.

Качество знаний характеризуется способностью обучающегося точно, структурированно и уместно воспроизводить информацию, полученную в процессе освоения дисциплины, в том виде, в котором она была изложена в учебном издании или преподавателем.

Умения, как правило, формируются на занятиях семинарского типа. Задания, направленные на оценку умений, в значительной степени требуют от обучающегося проявления стереотипности мышления, т.е. способности выполнить работу по образцам, с которыми он работал в процессе обучения. Преподаватель же оценивает своевременность и правильность выполнения задания.

Навыки можно трактовать как автоматизированные умения, развитые и закрепленные осознанным самостоятельным трудом. Навыки формируются при самостоятельном выполнении обучающимися практико-ориентированных заданий, моделирующих решение им производственных и социокультурных задач в соответствующей области профессиональной деятельности, как правило, при выполнении домашних заданий, курсовых проектов (работ), научно-исследовательских работ, прохождении практик, при работе индивидуально или в составе группы и т.д.

Устный опрос – это процедура, организованная как специальная беседа преподавателя с группой обучающихся (фронтальный опрос) или с отдельными обучающимися (индивидуальный опрос) с целью оценки сформированности у них основных понятий и усвоения учебного материала. Устный опрос может использоваться как вид контроля и метод оценивания формируемых компетенций (как и качества их формирования) в рамках самых разных форм контроля, таких как: собеседование, коллоквиум, зачет, экзамен по дисциплине. Устный опрос (УО) позволяет оценить знания и кругозор обучающегося, умение логически построить ответ, владение монологической речью и иные коммуникативные навыки. УО обладает большими возможностями воспитательного воздействия преподавателя. Воспитательная функция УО имеет ряд важных аспектов: профессионально-этический и нравственный аспекты, дидактический (систематизация материала при ответе, лучшее запоминание материала при интеллектуальной концентрации), эмоциональный (радость от успешного прохождения собеседования) и др. Обучающая функция УО состоит в выявлении деталей, которые по каким-то причинам оказались недостаточно осмысленными в ходе учебных занятий и при подготовке к зачёту или экзамену. УО обладает также мотивирующей функцией: правильно организованные собеседование, коллоквиум, зачёт и экзамен могут стимулировать учебную деятельность студента, его участие в научной работе.

Тесты являются простейшей формой контроля, направленной на проверку владения терминологическим аппаратом, современными информационными технологиями и конкретными

знаниями в области фундаментальных и прикладных дисциплин. Тест может предоставлять возможность выбора из перечня ответов (один или несколько правильных ответов).

Семинарские занятия. Основное назначение семинарских занятий по дисциплине – обеспечить глубокое усвоение обучающимися материалов лекций, прививать навыки самостоятельной работы с литературой, воспитывать умение находить оптимальные решения в условиях изменяющихся отношений, формировать современное профессиональное мышление обучающихся. На семинарских занятиях преподаватель проверяет выполнение самостоятельных заданий и качество усвоения знаний, умений, определяет уровень сформированности компетенций.

Коллоквиум может служить формой не только проверки, но и повышения производительности труда студентов. На коллоквиумах обсуждаются отдельные части, разделы, темы, вопросы изучаемого курса, обычно не включаемые в тематику семинарских и других практических учебных занятий, а также рефераты, проекты и иные работы обучающихся.

Доклад, сообщение – продукт самостоятельной работы студента, представляющий собой публичное выступление по представлению полученных результатов решения определенной учебно-практической, учебно-исследовательской или научной темы.

Контрольная работа - средство проверки умений применять полученные знания для решения задач определенного типа по теме или разделу.

Профессионально-ориентированное эссе – это средство, позволяющее оценить умение обучающегося письменно излагать суть поставленной проблемы, самостоятельно проводить анализ этой проблемы с использованием аналитического инструментария соответствующей дисциплины, делать выводы, обобщающие авторскую позицию по поставленной профессионально-ориентированной проблеме.

Реферат – продукт самостоятельной работы студента, представляющий собой краткое изложение в письменном виде полученных результатов теоретического анализа определенной научной (учебно-исследовательской) темы, где автор раскрывает суть исследуемой проблемы, приводит различные точки зрения, а также собственные взгляды на нее.

Ситуационный анализ – это комплексный анализ ситуации, имевший место в реальной практике профессиональной деятельности специалистов. Комплексный анализ включает в себя следующие составляющие: причинно-следственный анализ (установление причин, которые привели к возникновению данной ситуации, и следствий ее развертывания), системный анализ (определение сущностных предметно-содержательных характеристик, структуры ситуации, ее функций и др.), ценностно-мотивационный анализ (построение системы оценок ситуации, ее составляющих, выявление мотивов, установок, позиций действующих лиц); прогностический анализ (разработка перспектив развития событий по позитивному и негативному сценарию), рекомендательный анализ (выработка рекомендаций относительно поведения действующих лиц ситуации), программно-целевой анализ (разработка программ деятельности для разрешения данной ситуации).

Творческое задание – это частично регламентированное задание, имеющее нестандартное решение и позволяющее диагностировать умения интегрировать знания различных научных областей, аргументировать собственную точку зрения, доказывать правильность своей позиции. Может выполняться в индивидуальном порядке или группой обучающихся.

Деловая и/или ролевая игра – совместная деятельность группы обучающихся и преподавателя под управлением преподавателя с целью решения учебных и профессионально-ориентированных задач путем игрового моделирования реальной проблемной ситуации. Позволяет оценивать умение анализировать и решать типичные профессиональные задачи.

«Круглый стол», дискуссия – интерактивные оценочные средства, позволяющие включить обучающихся в процесс обсуждения спорного вопроса, проблемы и оценить их умение аргументировать собственную точку зрения. Занятие может проводить по традиционной (контактной) технологии, либо с использованием телекоммуникационных технологий.

Проект – конечный профессионально-ориентированный продукт, получаемый в результате планирования и выполнения комплекса учебных и исследовательских заданий. Позволяет оценить умения обучающихся самостоятельно конструировать свои знания в процессе решения практических задач и проблем, ориентироваться в информационном пространстве и уровень

сформированности аналитических, исследовательских навыков, навыков практического и творческого мышления. Может выполняться в индивидуальном порядке или группой обучающихся.

Раздел 8. Методические указания для обучающихся по освоению дисциплины

Для успешного освоения дисциплины студенту необходимо посещать все контактные занятия и систематически в полном объеме выполнять все задания для самостоятельной работы.

Во время лекций рекомендуется вести записи: выделять основные понятия, факты, выводы. Если какое-то объяснение кажется непонятным, следует немедленно задать вопрос преподавателю. Для формирования необходимых компетенций рекомендуется принимать активное участие в обсуждении ставящихся перед аудиторией вопросов.

При подготовке к лабораторным занятиям необходимо тщательно изучить теоретический и методический материал, изложенный в лекциях.

Самостоятельная работа студентов является одной из основных форм внеаудиторной работы при реализации учебных планов и программ. По дисциплине «Информационная безопасность» практикуются следующие виды и формы самостоятельной работы студентов:

- отработка изучаемого материала по печатным и электронным источникам, конспектам лекций;
- изучение лекционного материала по конспекту с использованием рекомендованной литературы;
- изучение тем, вынесенных на самостоятельную проработку;
- подготовка к лабораторным работам и оформление отчётов;
- подготовка информационных сообщений, докладов;
- подготовку к зачету.

Самостоятельная работа может проходить в лекционном кабинете, компьютерном зале, дома.

Основной формой работы студента по изучению дисциплины является изучение конспекта лекций, их дополнение, рекомендованной литературы, активное участие при выполнении лабораторных работ.

Все неясные вопросы по дисциплине обучающийся может уточнить у преподавателя. При подготовке к лабораторным работам обучающийся в обязательном порядке изучает теоретический материал в соответствии с перечнем основной учебной литературы и методическими указаниями.

Учебно-методическое обеспечение самостоятельной работы студентов по дисциплине включает:

1. Методические указания по дисциплине Информационная безопасность / составители А. Г. Ерохин. — Москва : Московский технический университет связи и информатики, 2013. — 20 с. — Текст : электронный // Цифровой образовательный ресурс IPR SMART : [сайт]. — URL: https://www.IPRsmart hop.ru/61736.html

2. Методические указания и индивидуальные задания для самостоятельной работы по дисциплине Комплексное обеспечение информационной безопасности инфокоммуникационных сетей и систем / составители И. Л. Боброва, К. А. Севрук. — Москва : Московский технический университет связи и информатики, 2015. — 35 с. — Текст : электронный // Цифровой образовательный ресурс IPR SMART : [сайт]. — URL: https://www.IPRsmart hop.ru/61737.html

Раздел 9. Учебно-методическое и информационное обеспечение дисциплины

Основная литература[1]

1. Галатенко, В. А. Основы информационной безопасности : учебное пособие / В. А. Галатенко. - 3-е изд. - Москва : Интернет-Университет Информационных Технологий (ИНТУИТ), Ай Пи Ар Медиа, 2020. - 266 с. - ISBN 978-5-4497-0675-1. - Текст : электронный // Цифровой образовательный ресурс IPR SMART : [сайт]. - URL: https://www.IPRsmart hop.ru/97562.html

[1] Из ЭБС

2. Башлы, П. Н. Информационная безопасность и защита информации : учебное пособие / П. Н. Башлы, А. В. Бабаш, Е. К. Баранова. — Москва : Евразийский открытый институт, 2012. — 311 с. — ISBN 978-5-374-00301-7. — Текст : электронный // Цифровой образовательный ресурс IPR SMART : [сайт]. — URL: https://www.IPRsmart hop.ru/10677.html

Дополнительная литература[2]

3. Фомин, Д. В. Информационная безопасность : учебное пособие для СПО / Д. В. Фомин. - Саратов, Москва : Профобразование, Ай Пи Ар Медиа, 2022. - 218 с. - ISBN 978-5-4488-1351-1, 978-5-4497-1565-4. - Текст : электронный // Цифровой образовательный ресурс IPR SMART : [сайт]. - URL: https://www.IPRsmart hop.ru/118458.html

4. Нестеров С.А., Основы информационной безопасности : учебное пособие / Нестеров С.А.. — Санкт-Петербург : Санкт-Петербургский политехнический университет Петра Великого, 2014. — 322 с. — ISBN 978-5-7422-4331-1. — Текст : электронный // Цифровой образовательный ресурс IPR SMART : [сайт]. — URL: https://www.IPRsmart hop.ru/43960.html

Перечень информационных технологий, используемых при осуществлении образовательного процесса по дисциплине: интернет-ресурсы, современные профессиональные базы данных, информационные справочные системы

Интернет-ресурсы

URL: https://www.IPRsmart hop.ru/ – электронно-библиотечная система IPRsmart .

Информационно-справочные и поисковые системы

Справочная правовая система «КонсультантПлюс»: http://www.con-sultant.ru

Современные профессиональные базы данных

URL:http://www.edu.ru/ – библиотека федерального портала «Российское образование»
URL:http://www.prlib.ru – Президентская библиотека
URL:http://www.rusneb.ru – Национальная электронная библиотека
URL:http://elibrary.rsl.ru/ – сайт Российской государственной библиотеки (раздел «Электронная библиотека»)
URL:http://elib.gnpbu.ru/ – сайт Научной педагогической электронной библиотеки им. К.Д. Ушинского

Комплект лицензионного и свободно распространяемого программного обеспечения, в том числе отечественного производства

Комплект лицензионного программного обеспечения

Microsoft Open Value Subscription для решений Education Solutions № Tr000544893 от 21.10.2020 г. MDE Windows, Microsoft Office и Office Web Apps. (срок действия до 01.11.2023 г.)

Антивирусное программное обеспечение ESET NOD32 Antivirus Business Edition договор № ИС00-006348 от 14.10.2022 г. (срок действия до 13.10.2025 г.)

Программное обеспечение «Мираполис» система вебинаров - Лицензионный договор 244/09/16-к от 15.09.2016 (Спецификация к Лицензионному договору 244/09/16-к от 15.09.2016, от 11.05.2022 г.) (срок действия до 10.07.2023 г.)

Электронная информационно-образовательная среда «1С: Университет» договор от 10.09.2018 г. №ПРКТ-18281 (бессрочно)

Информационная система «ПервыйБит» сублицензионный оговор от 06.11.2015 г. №009/061115/003 (бессрочно)

Система тестирования Indigo лицензионное соглашение (Договор) от 08.11.2018 г. №Д-54792 (бессрочно)

Информационно-поисковая система «Консультант Плюс» - договор об информационно поддержке от 26.12.2014, (бессрочно)

Электронно-библиотечная система IPRsmart лицензионный договор от 01.09.2021 г. №8234/21С (срок действия до 31.08.2024 г.)

Научная электронная библиотека eLIBRARY лицензионный договор SCIENC INDEX № SIO - 3079/2022 от 12.01.2022 г. (срок действия до 27.01.2024 г.)

[2] Из ЭБС

Свободно распространяемое программное обеспечение

Комплект онлайн сервисов GNU ImageManipulationProgram, свободно распространяемо программное обеспечение

Веб-браузер, Google Ghrome, свободное ПО, ежегодно обновляемое ПО.

Пакет офисных приложений, Office 2016, лицензионное соглашение - Договор №Tr000544893 от 21/10/2020 – 3 года

Пакет офисных приложений, OpenOffice, свободное ПО, ежегодно обновляемое ПО

Просмотр файлов в формате PDF, Adobe Reader, свободно распространяемое ПО, ежегодно обновляемое ПО

Просмотр файлов в формате DJV, WinDjView, свободное ПО, ежегодно обновляемое ПО

Файловый архиватор, 7 Zip, свободное ПО, ежегодно обновляемое ПО

Файловый менеджер, Far, свободно распространяемое ПО, ежегодно обновляемое ПО

Anaconda: дистрибутив языков программирования Python и R.

Программное обеспечение отечественного производства:

Программное обеспечение «Мираполис» система вебинаров - Лицензионный договор 244/09/16-к от 15.09.2016 (Спецификация к Лицензионному договору 244/09/16-к от 15.09.2016, от 11.05.2022 г.) (срок действия до 10.07.2023 г.)

Электронная информационно-образовательная среда «1С: Университет» договор от 10.09.2018 г. №ПРКТ-18281 (бессрочно)

Информационная система «ПервыйБит» сублицензионный договор от 06.11.2015 г. №009/061115/003 (бессрочно)

Система тестирования Indigo лицензионное соглашение (Договор) от 08.11.2018 г. №Д-54792 (бессрочно)

Информационно-поисковая система «Консультант Плюс» - договор МИ-ВИП-79717-56/2022 от 23.12.2021 (срок действия до 31.12.2022 г.)

Информационно-поисковая система «Консультант Плюс» - договор об информационно поддержке от 26.12.2014, (бессрочно)

Электронно-библиотечная система IPRsmart лицензионный договор от 01.09.2021 г. №8234/21С (срок действия до 31.08.2024 г.)

Научная электронная библиотека eLIBRARY лицензионный договор SCIENC INDEX № SIO -3079/2022 от 12.01.2022 г. (срок действия до 27.01.2024 г.)

ОБРАЗОВАТЕЛЬНОГО ПРОЦЕССА

Учебная аудитория для проведения занятий лекционного типа, занятий семинарского типа, групповых и индивидуальных консультаций, текущего контроля и промежуточной аттестации	Оборудование: специализированная мебель (мебель аудиторная (11 столов, 11 стульев, доска аудиторная), стол преподавателя, стул преподавателя. Технические средства обучения: персональный компьютер -11; мультимедийное оборудование (проектор, экран).
Помещение для самостоятельной работы	Специализированная мебель (10 столов, 10 стульев), персональные компьютеры с возможностью подключения к сети «Интернет» и обеспечением доступа в электронную информационно-образовательную среду Университета