Автономная образовательная некоммерческая организация
высшего образования
«Институт Бизнеса и Информационных Систем»
(АОНО ВО «ИБИС»)

Факультет Бизнеса и информационных систем
Кафедра Информационных технологий

УТВЕРЖДАЮ
Проректор по учебно-воспитательной работе
_____М.В. Доможирова
«12» 05 2023 г.

РАБОЧАЯ ПРОГРАММА И ОЦЕНОЧНЫЕ МАТЕРИАЛЫ

дисциплины

Б1.В.ДВ.03.01 «Информационная безопасность и защита информации»

Уровень образования:	Высшее образование – бакалавриат
Направление подготовки:	09.03.02 Информационные системы и технологии
Направленность (профиль):	Информационные системы и сетевые технологии
Форма обучения:	Очная, заочная
Составитель:	д.т.н. Мельников А.В.

Воронеж 2023 г.

Разработчик рабочей программы дисциплины: д.т.н. Мельников Александр Владимирович

Рабочая программа дисциплины рассмотрена и утверждена на заседаниях:

кафедры «Информационных технологий», протокол №2 от «24» апреля 2023 года.

Ученого совета АОНО «Институт Бизнеса и Информационных Систем», протокол № 3 от «11» мая 2023 года.

1. Цели и задачи учебной дисциплины

Цель освоения дисциплины «Информационная безопасность и защита информации»: является изучение основных принципов, методов и средств защиты информации в процессе ее обработки, передачи и хранения с использованием компьютерных средств в информационных системах

Задачи дисциплины:

– сформировать общее представление об информационной безопасности как о состоянии защищенности информационного ресурса сложной системы, понимание необходимости системного подхода к практической реализации такого состояния;

– передать знания о порядке организации и практической реализации типовых мероприятий по обеспечению информационной безопасности и защите информации;

– сформировать навыки анализа информационных ресурсов по следующим факторам: важность, конфиденциальность, уязвимость.

2. Место дисциплины в структуре ОПОП ВО

Дисциплина «Информационная безопасность и защита информации» относится к вариативной части дисциплин по выбору Блока 1 и ориентирована на обучающихся, имеющих начальную подготовку в рамках дисциплин: «Информатика», «Сети и телекоммуникации», «Инструментальные средства информационных систем», «Моделирование процессов и систем».

Дисциплина может быть использована при изучении дисциплин: «Администрирование сетевого оборудования», «Автоматизация проектирования информационных систем», в рамках практик, подготовки выпускной квалификационной работы

3. Перечень планируемых результатов обучения по дисциплине, соотнесенные с установленными в ОП ВО индикаторами достижения компетенций

Задача профессиональной деятельности	Код и наименование компетенции	Код и наименование индикатора достижения компетенции	Планируемые результаты обучения по дисциплине
Применение современных информационно-коммуникационных технологий процессе осуществления профессиональных функций	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 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.	Знает: основные нормативные правовые акты в области информационной безопасности и защиты информации; правовые основы организации защиты государственной тайны и конфиденциальной информации, задачи органов защиты государственной тайны; правовые нормы и стандарты по лицензированию в области обеспечения защиты государственной тайны и сертификации

			средств защиты информации; принципы и методы организационной защиты информации
		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.	Умеет Уметь: - применять правовые, организационные, технические и программные средства защиты информации - выявлять потенциальные каналы утечки информации и определять их характеристики - разрабатывать и обосновывать варианты эффективных управленческих решений в области информационной безопасности - систематизировать и обобщать информацию, готовить обзоры по вопросам информационной безопасности
		ОПК-3.3 Иметь навыки: подготовки обзоров, аннотаций, составления рефератов, научных докладов, публикаций и библиографии по научно-исследовательской работе с учетом требований информационной безопасности.	Владеет: - навыками противодействия утечке компьютерной информации - навыками использования электронной цифровой подписи - навыками проведения аудита локальной политики безопасности - специальной терминологией, применяемой в процессе защиты информации - навыками профессиональной аргументации при разборе стандартных ситуаций
Исследование моделей и методов	ПК-5 Способен к организации и про-	ПК-5.1 Знать: основные научные методи-	Знает: основные методики, лежащие в

информационных систем и технологий на базе современных программных пакетов моделирования, проектирования и автоматизации.	ведению экспериментальных исследований и компьютерного моделирования с применением современных средств и методов	ки, применяемые при разработке, внедрении и сопровождении информационных технологий и систем.	основе криптографических моделей
		ПК-5.2 Уметь: применять выбранные научно-исследовательские методики.	Умеет: использовать алгоритмические модели и языки программирования для разработки алгоритмов шифрования; выбирать, адаптировать и применять необходимые алгоритмы при решении профессиональных задач
		ПК-5.3. Имеет навыки анализа и критической оценки полученных результатов.	Владеет: навыками решения задач криптоанализа и шифрования.

4. Объем и структура дисциплины

Общая трудоемкость дисциплины составляет 3 з.е., 108 час.

Вид учебной работы	Формы обучения					
	Очная			Заочная		
	Всего часов	из них в семестре		Всего часов	из них в семестре	
		6			8	
Общая трудоемкость дисциплины	108	108		108	108	
Контактная работа обучающихся с преподавателем, всего	54	54		10	10	
в том числе:						
Лекции	18	18		4	4	
Лабораторные работы						
Практические занятия	36	36		6	6	
Самостоятельная работа	54	54		94	94	
Промежуточная аттестация (подготовка и сдача)	-	-		4	4	
Курсовая работа/проект	-	-		-	-	
Контрольная работа	-	-		-	-	
Промежуточная аттестация: экзамен/зачет/зачет с оценкой	Зачет	Зачет		Зачет	Зачет	

5. Содержание дисциплины, структурированное по темам (разделам) с указанием отведенного на них количества академических часов и видов учебных занятий

Содержание тем дисциплины, структурированное по темам с указанием дидактического материала по каждой изучаемой теме

№ п/п	Наименование темы	Содержание темы
1	Тема 1. Понятие и сущность информационной безопасности и защиты информации	Необходимость и значимость нормативно- правового определения основных понятий. Понятие информационной безопасности (ИБ) и защиты информации. Основные компоненты безопасности государства и доминирующая роль ИБ. Становление и развитие понятия «информационная безопасность». Связь ИБ с информатизацией общества. Базовые уровни обеспечения ИБ и защиты информации.
2	Тема 2. Основные угрозы информационной безопасности	Классификация угроз безопасности по цели реализации угрозы, принципу, характеру и способу её воздействия. Особенности угроз воздействия на объект атаки в зависимости от его состояния и используемых средств атаки. Основные методы и каналы несанкционированного доступа к информации в информационной системе (ИС). Базовые принципы защиты от несанкционированного доступа к информации в соответствии с нормативно-правовыми документами России. Задачи по защите ИС от реализации угроз.
3	Тема 3. Правовой уровень обеспечения информационной безопасности	Основные федеральные органы, генеририрующие в Российской Федерации нормативно-правовые акты в сфере ИБ и защиты информации. Роль в России Межведомственной комиссии по защите государственной тайны в формировании перечня сведений, составляющих государственную тайну. Место коммерческой тайны в системе предпринимательской деятельности. Основания и методика отнесения сведений к коммерческой тайне. Степени конфиденциальности сведений, составляющих коммерческую тайну. Методика формирования на фирме перечня. сведений, относящихся к коммерческой тайне.
4	Тема 4. Административный уровень обеспечения информационной безопасности	Концепция ИБ, её цели и этапы построения. Политика информационной безопасности (ПИБ) как основа административных мер по защите информации на предприятии. Структура документа, характеризующего политику безопасности, и основные этапы разработки политики ИБ. Задачи, решаемые при анализе рисков для ИС. Базовые методики, используемые для оценки рисков. Основные стандарты в области разработки ПИБ и

		анализа рисков. Базовые инструментальные средства для анализа рисков и управления рисками. Основные принципы реализации ПИБ.
5	Тема 5. Программно- технический уровень обеспечения защиты информации	Программные сервисы защиты информации в ИС. Идентификация и аутентификация пользователей как передовой рубеж защиты информации. Базовые методы парольной аутентификации. Модели разграничения доступа к информации. Протоколирование и аудит (активный и пассивный) ИС, их основные цели и особенности. Базовые методы криптографического преобразования данных. Потоковое и блочное шифрование. Процедура формирования электронной подписи. Экранирование информации в информационно- телекоммуникационных сетях (ИТС). Основные сервисы защиты в ИТС. Компьютерные вирусы и вредоносные программы: классификация, методы и средства борьбы с ними. Антивирусные программные комплексы.
6	Тема 6. Процедурный уровень информационной безопасности	Основные классы мер процедурного уровня. Управление персоналом. Физическая защита. Поддержание работоспособности. Реагирование на нарушения режима безопасности. Планирование восстановительных работ
7	Тема 7. Система защиты информации	Процесс развития средств и методов защиты информации. Этапы развития системы защиты информации в настоящее время. Комплексный подход к построению системы защиты информации. Системный подход к построению системы защиты информации. Цели задачи системы защиты информации. Этапы и порядок проведения работ по созданию системы защиты информации. Структура систем защиты информации на современном этапе. Методы (виды) обеспечения защиты информации.
8	Тема 8. Обеспечение режима конфиденциальности при работе с защищаемой информацией	Разрешительная (разграничительная) система доступа должностных лиц, работников к конфиденциальным сведениям, документам и базам данных Допуск должностных лиц, работников к конфиденциальной информации. Доступ должностных лиц, работников к конфиденциальным сведениям, документам и базам данных. Обязанности должностных лиц, допущенных к сведениям, составляющим коммерческую тайну Порядок предоставления (получения) конфиденциальной информации работникам сторонних организаций, государственным учреждениям
9	Тема 9. Контроль за соблюдением требований информационной безопасности и защиты информации	Основные положения по осуществлению контроля, назначение, цель и задачи контроля. Основные мероприятия по осуществлению контроля. Порядок проведения проверки (контроля) наличия документов и иных носителей информации ограниченного доступа. Проведение служебного расследо-

		вания по фактам утечки конфиденциальной информации, утраты носителей, содержащих такие сведения, а также по фактам грубых нарушений режима конфиденциальности.

Тематический план (очная форма обучения)

№ п/п	Наименование тем	Всего часов по учебному плану	Контактная работа с преподавателем:					Самостоятельная работа
			Всего часов	Лекции	Занятия семинарского типа			
					Семинарские занятия	Практические занятия	Другие виды занятий	
6 семестр								
1	Тема 1. Понятие и сущность информационной безопасности и защиты информации	12	6	2		4		6
2	Тема 2. Основные угрозы информационной безопасности	12	6	2		4		6
3	Тема 3. Правовой уровень обеспечения информационной безопасности	12	6	2		4		6
4	Тема 4. Административный уровень обеспечения информационной безопасности	12	6	2		4		6
5	Тема 5. Программно- технический уровень обеспечения защиты информации	12	6	2		4		6
6	Тема 6. Процедурный уровень информационной безопасности	12	6	2		4		6
7	Тема 7. Система защиты информации	12	6	2		4		6
8	Тема 8. Обеспечение режима конфиденциальности при работе с защищаемой информацией	12	6	2		4		6
9	Тема 9. Контроль за соблюдением требований информационной безопасности и защиты информации	12	6	2		4		6
Форма контроля: Зачет								
Итого за семестр		108	54	18		36		54

Тематический план (заочная форма обучения)

№ п/п	Наименование тем	Всего часов по учебному плану	Контактная работа с преподавателем:					Самостоятельная работа
			Всего часов	Лекции	Занятия семинарского типа			
					Семинарские занятия	Практические занятия	Другие виды занятий	
8 семестр								
1	Тема 1. Понятие и сущность информационной безопасности и защиты информации	12	2	2				10
2	Тема 2. Основные угрозы информационной безопасности	12	2			2		10
3	Тема 3. Правовой уровень обеспечения информационной безопасности	10						10
4	Тема 4. Административный уровень обеспечения информационной безопасности	12	2			2		10
5	Тема 5. Программно- технический уровень обеспечения защиты информации	12	2	2				10
6	Тема 6. Процедурный уровень информационной безопасности	10						10
7	Тема 7. Система защиты информации	12	2			2		10
8	Тема 8. Обеспечение режима конфиденциальности при работе с защищаемой информацией	12						12
9	Тема 9. Контроль за соблюдением требований информационной безопасности и защиты информации	12						12
Форма контроля: Зачет		4						4
Итого за семестр		**108**	**10**	**4**		**6**		**98**

6. Самостоятельная работа обучающихся в ходе освоения дисциплины

№ п/п	Вид самостоятельной работы	Наименование работы и содержание
1	Освоение учебного материала по конспекту лекций и дополнительной литературе	Доработать конспект, желательно в тот же день. Прочитать записи, восстановить текст в памяти, а также исправить описки, расшифровать не принятые ранее сокращения, заполнить пропущенные места, понять текст, вникнуть в его смысл. Изучить материал, используя рекомендуемую литературу, разрешая в ходе чтения, возникшие

		ранее затруднения, находя ответы на вопросы, а также дополняя и исправляя свои записи. Записи должны быть наглядными, для чего следует применять различные способы выделений. Подготовленный конспект и рекомендуемая литература используются при подготовке к практическому занятию.
2	Подготовка к практическим занятиям	Подготовка к практическому занятию включает следующие элементы самостоятельной деятельности: четкое представление цели и задач его проведения; выделение навыков умственной, аналитической деятельности, которые станут результатом предстоящей работы. Выработка навыков осуществляется с помощью получения новой информации об изучаемых процессах и с помощью знания о том, в какой степени в данное время студент владеет методами исследовательской деятельности, которыми он станет пользоваться на практическом занятии.
3	Изучение основной и дополнительной литературы	Самостоятельная работа с учебниками и книгами (а также самостоятельное теоретическое исследование проблем, обозначенных преподавателем на лекциях) – это важнейшее условие познания. В самостоятельной работе рекомендуется прибегать к таким видам систематизированной записи прочитанного как аннотирование, тезирование, цитирование, конспектирование. Причем конспект аккумулирует в себе предыдущие виды записи, позволяет всесторонне охватить содержание книги, статьи. Поэтому умение составлять план, тезисы, делать выписки и другие записи определяет и технологию составления конспекта.
4	Подготовка к зачету	Необходимо перечитать лекции, вспомнить то, что говорилось преподавателем на семинарах и практических занятиях, а также самостоятельно полученную ин формацию при подготовке к ним. важно сформировать целостное представление о содержании ответа на каждый вопрос, что предполагает знание разных научных трактовок сущности того или иного явления, процесса, умение раскрывать факторы, определяющие их противоречивость, знание имен ученых, изучавших обсуждаемую проблему. необходимо также привести информацию о материалах эмпирических исследований, что указывает на всестороннюю подготовку студента к зачету. ответ, в котором присутствуют все указанные блоки информации, наверняка будет отмечен высокими баллами. для их получения требуется ответить и на дополнительные вопросы, если зачет проходит в устной форме. Рекомендуется подготовку к зачету осуществлять в два этапа. На первом, в течение 2–3 дней, подбирается из разных источников весь материал, необходимый для развернутых ответов на все вопросы. ответы можно записать в виде краткого конспекта. На втором этапе по памяти восстанавливается содержание того, что записано в ответах на каждый вопрос.

7. Фонд оценочных средств для текущей и промежуточной аттестации по дисциплине

Оценочные средства для проведения текущей и промежуточной аттестации

Код контролируемого индикатора освоения компетенции	Наименование оценочного средства для проведения текущей аттестации	Наименование оценочного средства для проведения промежуточной аттестации
ОПК-3.1, ОПК-3.2, ОПК-3.3 ПК-5.1, ПК-5.2, ПК-5.3	контрольные вопросы, тестовые задания, практические работы	Зачет

Критерии оценивания результата обучения по дисциплине и шкала оценивания

Код контролируемой компетенции	Критерии оценивания результата обучения по дисциплине и шкала оценивания			
	неудовлетворительно	удовлетворительно	хорошо	отлично
	Не зачтено	Зачтено		
ОПК-3	Отсутствие или фрагментарные способности решать стандартные задачи профессиональной деятельности на основе информационной и библиографической культуры с применением информационно-коммуникационных технологий	Неполные способности решать стандартные задачи профессиональной деятельности на основе информационной и библиографической культуры с применением информационно-коммуникационных технологий	Сформированные, но содержащие отдельные пробелы способности решать стандартные задачи профессиональной деятельности на основе информационной и библиографической культуры с применением информационно-коммуникационных технологий	Сформированные систематические решать стандартные задачи профессиональной деятельности на основе информационной и библиографической культуры с применением информационно-коммуникационных технологий
ПК-5	обучающийся обнаруживает незнание ответа на соответствующее задание, допускает принципиальные ошибки в формулировке определений и правил, в тече-	обучающийся демонстрирует удовлетворительное, но не систематизированное владение способностями к организации и проведению экспериментальных иссле-	обучающийся демонстрирует достаточно полное, с небольшими неточностями, владение способностями к организации и проведению эксперимен-	обучающийся демонстрирует полное, систематизированное владение способностями к организации и проведению экспериментальных исследований и ком-

	ние семестра не сформировал необходимых умений и навыков	дований и компьютерного моделирования с применением современных средств и методов	тальных исследований и компьютерного моделирования с применением современных средств и методов	пьютерного моделирования с применением современных средств и методов

8. Ресурсное обеспечение учебной дисциплины

Основная литература:

1. Сычев, Ю. Н. Защита информации и информационная безопасность : учебное пособие / Ю.Н. Сычев. — Москва : ИНФРА-М, 2022. — 201 с. — (Высшее образование: Бакалавриат). — DOI 10.12737/1013711. - ISBN 978-5-16-014976-9. - Текст : электронный. - URL: https://znanium.com/catalog/product/1844364 (дата обращения: 20.12.2021). – Режим доступа: по подписке.

Дополнительная литература:

1. Баранова, Е. К. Информационная безопасность и защита информации : учебное пособие / Е.К. Баранова, А.В. Бабаш. — 4-е изд., перераб. и доп. — Москва : РИОР : ИНФРА-М, 2021. — 336 с. — (Высшее образование). — DOI: https://doi.org/10.29039/1761-6. - ISBN 978-5-369-01761-6. - Текст : электронный. - URL: https://znanium.com/catalog/product/1189326 (дата обращения: 20.12.2021). – Режим доступа: по подписке.

2. Клименко, И. С. Информационная безопасность и защита информации: модели и методы управления : монография / И.С. Клименко. — Москва : ИНФРА-М, 2021. — 180 с. — (Научная мысль). — DOI 10.12737/monography_5d412ff13c0b88.75804464. - ISBN 978-5-16-015149-6. - Текст : электронный. - URL: https://znanium.com/catalog/product/1137902 (дата обращения: 20.12.2021). – Режим доступа: по подписке.

3. Башлы, П. Н. Информационная безопасность и защита информации [Электронный ресурс] : учебник / П. Н. Башлы, А. В. Бабаш, Е. К. Баранова. - Москва : РИОР, 2013. - 222 с. - ISBN 978-5-369-01178-2. - Текст : электронный. - URL: https://znanium.com/catalog/product/405000 (дата обращения: 20.12.2021). – Режим доступа: по подпис

4. Бахаров, Л. Е. Информационная безопасность и защита информации : разделы криптография и стеганография : практикум / Л. Е. Бахаров. - Москва : Изд. Дом НИТУ «МИСиС», 2019. - 59 с. - ISBN 978-5-906953-94-0. - Текст : электронный. - URL: https://znanium.com/catalog/product/1232734 (дата обращения: 20.12.2021). – Режим доступа: по подписке.

5. Бахаров, Л. Е. Информационная безопасность и защита информации : сборник тестов / Л. Е. Бахаров. - Москва : Изд. Дом МИСиС, 2015. - 43 с. - Текст : электронный. - URL: https://znanium.com/catalog/product/1232263 (дата обращения: 20.12.2021). – Режим доступа: по подписке.

Электронные ресурсы:

1. Федеральная служба государственной статистики [Электронный ресурс]. – Режим доступа: http://www.gks.ru/, свободный (дата обращения 30.09.2021Интернет Университет Информационных технологий. [Электронный ресурс] : сайт. – Режим доступа: http://www.intuit.ru/, свободный (дата обращения 30.09.2021

2. eLIBRARY.RU [Электронный ресурс] : научная электронная библиотека. – Режим доступа: http://elibrary.ru/defaultx.asp, свободный (дата обращения: 30.09.2021).

3. Информационные системы и технологии : [сайт]. – URL: https://studfiles.net/preview/4171546/page:4/ (дата обращения: 25.09.2021). – Режим доступа : свободный. – Текст : электронный.

4. Портал Федеральных государственных образовательных стандартов высшего образования: [сайт]. – URL: http://fgosvo.ru. (дата обращения: 25.09.2021). – Режим доступа : свободный. – Текст : электронный.

5. Федеральный центр информационно-образовательных ресурсов (ФЦИОР): [сайт]. – URL: http://edu.ru (дата обращения: 25.09.2021). – Режим доступа : свободный. – Текст : электронный.

6. Единая коллекция цифровых образовательных ресурсов (Единая коллекция ЦОР) : [сайт]. – URL: http://school-collection.edu.ru (дата обращения: 25.09.2021). – Режим доступа : свободный. – Текст : электронный.

7. Информационная система «Единое окно доступа к образовательным ресурсам» (ИС «Единое окно») : [сайт]. – URL: http://window/edu.ru (дата обращения: 25.09.2021). – Режим доступа : свободный. – Текст : электронный.

9. Материально-техническое обеспечение дисциплины

Учебная аудитория № 224 -учебная аудитория для проведения занятий лекционного типа; -учебная аудитория для проведения занятий семинарского тип и практических занятий; -учебная аудитория групповых и индивидуальных консультаций; -учебная аудитория для проведения текущего контроля и промежуточной аттестации. Оснащение оборудованием и техническими средствами обучения: - комплект учебной мебели для обучающихся; - рабочее место преподавателя; -доска меловая; -переносное видеопроекционное оборудование для мультимедиа презентации, средства звуковоспроизведения (персональный компьютер, проектор, экран, колонки). Лицензионное программное обеспечение: 1) иностранного производства: - MS Windows 7; - Microsoft Office Standard 2007. 2) отечественного производства: - Kaspersky EndPoint Security для Windows. Доступ к информационно-телекоммуникационной сети «Интернет» и к электронной информационно-образовательной среде организации.	394026, Воронежская область, г. Воронеж, ул. Дружинников, д.8 Кабинет № 224 (2 этаж № 3)
Учебная аудитория № 313 -учебная аудитория для проведения занятий лекционного типа; -учебная аудитория для проведения занятий семинарского тип и	394036, город Воронеж, ул. Карла Маркса, д.67

практических занятий; -учебная аудитория групповых и индивидуальных консультаций; -учебная аудитория для проведения текущего контроля и промежуточной аттестации; -учебная аудитория для курсового проектирования (выполнения курсовых работ); -компьютерный класс; -помещение для самостоятельной работы обучающихся. Оснащение оборудованием и техническими средствами обучения: -автоматизированное рабочее место обучающегося; -автоматизированное рабочее место преподавателя; -доска маркерная; - стационарное видеопроекционное оборудование для мультимедиа презентации, средства звуковоспроизведения (экран, проектор, колонки). Лицензионное программное обеспечение: 1) иностранного производства: - MS Windows 10; - Microsoft Office Standard 2007; - MS Visio; - MS Access 2016; - MS Project; - Microsoft SQL Server 2019; - Visual Studio 2010. 2) отечественного производства: - Kaspersky EndPoint Security для Windows. Свободно распространяемое программное обеспечение иностранного производства: - PascalABC.NET; - FreePascal IDE; - Eclipse; - IntelliJ IDEA; - GIMP; - Blender; - Firefox; - Vuze; - FileZilla; - Denver; - Maxima + WxMaxima, iTest; - Inkscape; - QCad. Российская информационная справочная правовая система «Консультант Плюс». Доступ к информационно-телекоммуникационной сети «Интернет» и к электронной информационно-образовательной среде организации.	Кабинет № 313 (3 этаж № 62)
Учебная аудитория № 318 -учебная аудитория для проведения занятий лекционного типа; -учебная аудитория для проведения занятий семинарского тип и практических занятий; -учебная аудитория групповых и индивидуальных консультаций;	394026, Воронежская область, г. Воронеж, ул. Дружинников, д.8 Кабинет № 318 (3 этаж № 50)

-учебная аудитория для проведения текущего контроля и промежуточной аттестации; -учебная аудитория для курсового проектирования (выполнения курсовых работ); -компьютерный класс; -помещение для самостоятельной работы обучающихся. Оснащение оборудованием и техническими средствами обучения: -автоматизированное рабочее место обучающегося; -автоматизированное рабочее место преподавателя; -доска двусторонняя (маркерно-меловая). - переносное видеопроекционное оборудование для мультимедиа презентации (ноутбук, проектор, экран, колонки). Лицензионное программное обеспечение: 1) иностранного производства: - MS Windows 7; - Microsoft Office Standard 2007; - MS Visio 2007; - MS Project 2010; - Microsoft SQL Server 2012; - Microsoft Visual Studio. 2) отечественного производства: - Kaspersky EndPoint Security для Windows; - Автоматизированная банковская система «Управление кредитной организацией» для ВУЗов. Свободно распространяемое программное обеспечение: 1) иностранного производства: - PascalABC.NET; - FreePascal IDE; - GIMP; - Blender; - Firefox; - Vuze; - FileZilla; - Denver; - Maxima + WxMaxima; - iTest; - Inkscape; - QCad; 2) отечественного производства: - программа Фоторобот. Российская информационная справочная правовая система «Консультант Плюс». Доступ к информационно-телекоммуникационной сети «Интернет» и к электронной информационно-образовательной среде организации.	
Помещение для самостоятельной работы обучающихся № 102 - помещение для самостоятельной работы обучающихся с доступом к сети «Интернет» и электронной информационно-образовательной среде организации; - читальный зал библиотеки - учебная аудитория для курсового проектирования (выполнения	394026, Воронежская область, г. Воронеж, ул. Дружинников, д.8 Кабинет № 102 (1 этаж № 84)

курсовых работ); -учебная аудитория для выполнения и защиты выпускной квалификационной работы. Оснащение оборудованием и техническими средствами обучения: -автоматизированное рабочее место обучающегося; - ноутбуки; - телевизор; - столы для чтения; - стулья; - шкафы для документов; -стол офисный; - стеллажи для книг; -стойка выдачи литературы; -тумба напольная; -информационная стойка. Лицензионное программное обеспечение: 1) иностранного производства: - MS Windows 7 pro; - Microsoft Office Standard 2007; - MS Access 2016. 2) отечественного производства: - Kaspersky EndPoint Security для Windows; Свободно распространяемое программное обеспечение: - 7-Zip; - Интернет цензор. Российская информационная справочная правовая система «Консультант Плюс». Доступ к информационно-телекоммуникационной сети «Интернет» и к электронной информационно-образовательной среде организации	
Учебная аудитория № 314 - помещение для самостоятельной работы обучающихся с доступом к сети «Интернет» и электронной информационно-образовательной среде организации; -учебная аудитория для курсового проектирования (выполнения курсовых работ); -учебная аудитория для выполнения выпускной квалификационной работы; - компьютерный класс. Оснащение оборудованием и техническими средствами обучения: -автоматизированное рабочее место обучающегося; -автоматизированное рабочее место преподавателя; -доска двусторонняя (маркерно - меловая); -наушники; -принтер; -телевизор. Лицензионное программное обеспечение: 1) иностранного производства: - MS Windows 8.1 Корпоративная; - Microsoft Office Standard 2007;	394026, Воронежская область, г. Воронеж, ул. Дружинников, д.8 Кабинет № 314 (3 этаж № 48)

- iSpring suite 8; - MS Visio; - MS Access 2016; - MS Project; - Microsoft SQL Server 2014; - Visual Studio 2017. 2) отечественного производства: - Kaspersky EndPoint Security для Windows; -1С: Предприятия 8. Комплект для обучения в высших и средних учебных заведениях. Свободно распространяемое программное обеспечение иностранного производства: - PascalABC.NET; - FreePascal IDE; - Eclipse; - IntelliJ IDEA; - GIMP; - Blender; - Firefox; - Vuze; - FileZilla; - Denver, Maxima + WxMaxima; - iTest; - Inkscape; - QCad. Информационная справочная правовая система «Консультант Плюс». Доступ к информационно-телекоммуникационной сети «Интернет» и к электронной информационно-образовательной среде организации.	
Учебная аудитория № 318 - помещение для самостоятельной работы обучающихся с доступом к сети «Интернет» и электронной информационно-образовательной среде организации; -учебная аудитория для курсового проектирования (выполнения курсовых работ); -учебная аудитория для выполнения выпускной квалификационной работы; Оснащение оборудованием и техническими средствами обучения: -автоматизированное рабочее место обучающегося; - автоматизированное рабочее место преподавателя; -доска двусторонняя (маркерно-меловая); - переносное видеопроекционное оборудование для мультимедиа презентации (ноутбук, проектор, экран, колонки). Лицензионное программное обеспечение: 1) иностранного производства: - MS Windows 7; - Microsoft Office Standard 2007; - MS Visio 2007; - MS Project 2010; - Microsoft SQL Server 2012;	394026, Воронежская область, г. Воронеж, ул. Дружинников, д.8 Кабинет № 318 (3 этаж № 50)

- Microsoft Visual Studio. 2) отечественного производства: - Kaspersky EndPoint Security для Windows; -Автоматизированная банковская система «Управление кредитной организацией» для ВУЗов. Свободно распространяемое программное обеспечение: 1) иностранного производства: - PascalABC.NET; - FreePascal IDE; - GIMP; - Blender; - Firefox; - Vuze; - FileZilla; - Denver; - Maxima + WxMaxima; - iTest; - Inkscape; - QCad; 2) отечественного производства: - программа Фоторобот. Российская информационная справочная правовая система «Консультант Плюс». Доступ к информационно-телекоммуникационной сети «Интернет» и к электронной информационно-образовательной среде организации.	
Учебная аудитория № 313 - помещение для самостоятельной работы обучающихся с доступом к сети «Интернет» и электронной информационно-образовательной среде организации; -учебная аудитория для курсового проектирования (выполнения курсовых работ); -учебная аудитория для выполнения выпускной квалификационной работы; - компьютерный класс. Оснащение оборудованием и техническими средствами обучения: -автоматизированное рабочее место обучающегося; - автоматизированное рабочее место преподавателя; -доска маркерная; - стационарное видеопроекционное оборудование для мультимедиа презентации, средства звуковоспроизведения (экран, проектор, колонки). Лицензионное программное обеспечение: 1) иностранного производства: - MS Windows 10; - Microsoft Office Standard 2007; - MS Visio; - MS Access 2016; - MS Project; - Microsoft SQL Server 2019; - Visual Studio 2010;	394036, город Воронеж, ул. Карла Маркса, д.67 Кабинет № 313 (3 этаж № 62)

2) отечественного производства: - Kaspersky EndPoint Security для Windows. Свободно распространяемое программное обеспечение иностранного производства: - PascalABC.NET; - FreePascal IDE; - Eclipse; - IntelliJ IDEA; - GIMP; - Blender; - Firefox; - Vuze; - FileZilla; - Denver; - Maxima + WxMaxima, iTest; - Inkscape; - QCad. Российская информационная справочная правовая система «Консультант Плюс». Доступ к информационно-телекоммуникационной сети «Интернет» и к электронной информационно-образовательной среде организации.	
Учебная аудитория № 314 - помещение для самостоятельной работы обучающихся с доступом к сети «Интернет» и электронной информационно-образовательной среде организации; -учебная аудитория для курсового проектирования (выполнения курсовых работ); -учебная аудитория для выполнения выпускной квалификационной работы; - компьютерный класс. Оснащение оборудованием и техническими средствами обучения: -автоматизированное рабочее место обучающегося; - автоматизированное рабочее место преподавателя; -доска двусторонняя (маркерно - меловая); -наушники; -принтер; -телевизор. Лицензионное программное обеспечение: 1) иностранного производства: - MS Windows 8.1 Корпоративная; - Microsoft Office Standard 2007; - iSpring suite 8; - MS Visio; - MS Access 2016; - MS Project; - Microsoft SQL Server 2014; - Visual Studio 2017. 2) отечественного производства: - Kaspersky EndPoint Security для Windows; -1С: Предприятия 8. Комплект для обучения в высших и средних	394036, город Воронеж, ул. Карла Маркса, д.67 Кабинет № 314 (3 этаж № 61)

учебных заведениях. Свободно распространяемое программное обеспечение иностранного производства: - PascalABC.NET; - FreePascal IDE; - Eclipse; - IntelliJ IDEA; - GIMP; - Blender; - Firefox; - Vuze; - FileZilla; - Denver, Maxima + WxMaxima; - iTest; - Inkscape; - QCad. Информационная справочная правовая система «Консультант Плюс». Доступ к информационно-телекоммуникационной сети «Интернет» и к электронной информационно-образовательной среде организации.	

10. Оценочные материалы для проведения текущего контроля и промежуточной аттестации обучающихся по дисциплине

10.1 Материалы для текущего контроля освоения дисциплины

Тема 1. Понятие и сущность информационной безопасности и защиты информации

Контрольные вопросы:

1. Современное состояние информационных технологий. Проблема защиты информации и этапы ее возможного решения.
2. Понятие ИБ. Объекты, цели и задачи ЗИ. Составляющие ИБ.
3. Распространение объектно-ориентированного подхода на ИБ.
4. Техническое обеспечение информационной безопасности.

Практическая работа №1 Защита документов MS Office

Цель: изучить методы защиты документов MS Office, правила создания сложных паролей

Вопросы по практической работе:

1. Опишите алгоритм задания пароля на открытие документа в MS Word
2. Опишите алгоритм задания пароля на изменение документа в MS Word
3. Опишите алгоритм задания пароля на открытие книги в MS Excel
4. Как защитить ячейку, лист, скрыть лист?
5. Как отменить пароли в документах MS Word, MS Excel?
6. Как установить пароли (на открытие, на изменение) в документах MS Office?
7. Перечислите правила создания паролей.

Тема 2. Основные угрозы информационной безопасности

Контрольные вопросы:

1. Угрозы ИБ: основные понятия. Виды и классификация угроз.
2. Основные угрозы целостности, конфиденциальности, доступности.
3. Виды мер обеспечения ИБ.
4. Защита информации в сети.
5. Задачи по защите ИС от реализации угроз

Практическая работа №2 Работа с программой вскрытия паролей AZPR

Цель: изучить возможности защиты архива паролем, научиться использовать программу вскрытия паролей Advanced ZIP Password Recovery

Вопросы по практической работе:

1. Какие виды атак на пароль Вы знаете?
2. Что такое плохой пароль?
3. Как можно противостоять атаке полным перебором?
4. Как длина пароля влияет на вероятность раскрытия пароля?
5. Какие рекомендации по составлению паролей Вы можете дать?

Тема 3. Правовой уровень обеспечения информационной безопасности

Контрольные вопросы:

1. Обзор российского законодательства в области защиты информации.
2. Федеральный закон «Об информации, информационных технологиях и о защите информации».
3. Место коммерческой тайны в системе предпринимательской деятельности.
4. Основания и методика отнесения сведений к коммерческой тайне.
5. Степени конфиденциальности сведений, составляющих коммерческую тайну.
6. Методика формирования на фирме перечня. сведений, относящихся к коммерческой тайне.

Практическая работа №3 Исследование и настройка межсетевого экрана

Цель: изучение механизмов работы средств обеспечения и поддержки сетевой защиты – брандмауэра и сетевого сканера; практическое ознакомление с работой сетевого сканера XSpider и межсетевого экрана Outpost

Вопросы по практической работе:

1. Опишите утилиту ping, методы и случаи ее применения.
2. Описать данные, полученные о компьютере напарника с помощью XSpider
3. Какого типа уязвимости были найдены?
4. Как можно предотвратить появление таких уязвимостей с помощью изученных средств?
5. Какие еще сканеры и МСЭ вы знаете? Какие между ними и изученными отличия?

Тема 4. Административный уровень обеспечения информационной безопасности

Контрольные вопросы:

1. Политика информационной безопасности (ПИБ) как основа административных мер по защите информации на предприятии.
2. Структура документа, характеризующего политику безопасности, и основные этапы разработки политики ИБ.
3. Задачи, решаемые при анализе рисков для ИС. Базовые методики, используемые для оценки рисков.
4. Основные стандарты в области разработки ПИБ и анализа рисков.
5. Базовые инструментальные средства для анализа рисков и управления рисками.
6. Основные принципы реализации ПИБ.

Практическая работа №4 Резервное копирование программ, системных параметров и файлов

Цель: изучить возможности резервного копирования в ОС Windows 7

Вопросы по практической работе:

1. Перечислите типы архивации и их возможности, которые можно выполнить с помощью элемента Панели управления Архивация и восстановление
2. Перечислите варианты размещения резервной копии файлов
3. Опишите алгоритм создания резервной копии файлов
4. Опишите алгоритм создания резервной копии образа системы
5. Опишите возможности использования диалогового окна Управление пространством
6. Перечислите рекомендации по резервному копированию

Тема 5. Программно- технический уровень обеспечения защиты информации

Контрольные вопросы:

1. Идентификация и аутентификация пользователей как передовой рубеж защиты информации.
2. Базовые методы парольной аутентификации.
3. Модели разграничения доступа к информации.
4. Протоколирование и аудит (активный и пассивный) ИС, их основные цели и особенности.
5. Базовые методы криптографического преобразования данных.
6. Потоковое и блочное шифрование.
7. Процедура формирования электронной подписи.
8. Экранирование информации в информационно- телекоммуникационных сетях (ИТС).
9. Основные сервисы защиты в ИТС.
10. Компьютерные вирусы и вредоносные программы: классификация, методы и средства борьбы с ними. Антивирусные программные комплексы

Практическая работа №5 Использование методов замены для шифрования данных

Цель: изучить классические шифры замены, научиться зашифровывать тексты с помощью шифров замены

Вопросы по практической работе:

1. Опишите алгоритм шифра Цезаря
2. Опишите алгоритм шифра Тритемиуса
3. Опишите правила шифрования по таблице Вижинера
4. Опишите правила расшифровки по таблице Вижинера
5. К какому классу шифров относятся перечисленные шифры?

Тема 6. Процедурный уровень информационной безопасности

Контрольные вопросы:

1. Основные классы мер процедурного уровня.
2. Управление персоналом.
3. Физическая защита.
4. Поддержание работоспособности.
5. Реагирование на нарушения режима безопасности.
6. Планирование восстановительных работ

Практическая работа №6 Использование методов перестановки для шифрования данных

Цель: изучить классические шифры перестановки, научиться зашифровывать тексты с помощью шифров перестановки, познакомиться с основами криптоанализа

Вопросы по практической работе:

1. Опишите простейшие примеры шифров перестановки
2. Опишите суть метода перестановки с ключом

3. Опишите суть метода шифрования перестановкой с пропусками (пробелами)
4. Опишите суть метода маршрутной перестановки
5. Возможен ли криптоанализ шифров перестановки, в чем его суть?

Тема 7. Система защиты информации

Контрольные вопросы:

1. Процесс развития средств и методов защиты информации.
2. Этапы развития системы защиты информации в настоящее время.
3. Комплексный подход к построению системы защиты информации.
4. Системный подход к построению системы защиты информации.
5. Этапы и порядок проведения работ по созданию системы защиты информации.
6. Структура систем защиты информации на современном этапе.
7. Методы (виды) обеспечения защиты информации

Практическая работа №7 Методы криптоанализа классических шифров

Цель: познакомиться с основами криптоанализа шифров перестановки

Вопросы по практической работе:

1. Что такое криптоанализ?
2. Опишите метод криптоанализа шифра столбцовой перестановки
3. Опишите метод криптоанализа шифра двойной перестановки
4. Какие дополнительные сведения желательно использовать при криптоанализе?

Тема 8. Обеспечение режима конфиденциальности при работе с защищаемой информацией

Контрольные вопросы:

1. Допуск должностных лиц, работников к конфиденциальной информации.
2. Доступ должностных лиц, работников к конфиденциальным сведениям, документам и базам данных.
3. Обязанности должностных лиц, допущенных к сведениям, составляющим коммерческую тайну
4. Порядок предоставления (получения) конфиденциальной информации работникам сторонних организаций, государственным учреждениям

Практическая работа №8 Шифрование с помощью аналитических преобразований

Цель: изучить методы алгебры матриц при шифровании сообщений

Вопросы по практической работе:

1. Опишите алгоритм шифрования текста с помощью матрицы
2. Опишите алгоритм дешифрования текста с помощью матрицы-ключа
3. Как вычислить определитель матрицы третьего порядка?
4. Как вычислить алгебраические дополнения к элементам матрицы?
5. Как вычислить обратную матрицу?
6. Матрицу какого порядка можно использовать при шифровании слов:

– ИГРА, ШИФР, КЛЮЧ;
– ЧУДЕСА, ПОЛИТИКА, ФЕОДОСИЯ, ЖЕРТВОПРИНОШЕНИЕ;
– НЕБЕСА, ЗВЕЗДОЧЕТ, КОНЦЕНТРАЦИЯ, ХРОМОЛИТОГРАФИЯ

Тема 9. Контроль за соблюдением требований информационной безопасности и защиты информации

Контрольные вопросы:

1. Основные положения по осуществлению контроля, назначение, цель и задачи контроля.
2. Основные мероприятия по осуществлению контроля.
3. Порядок проведения проверки (контроля) наличия документов и иных носителей информации ограниченного доступа.

4. Проведение служебного расследования по фактам утечки конфиденциальной информации, утраты носителей, содержащих такие сведения, а также по фактам грубых нарушений режима конфиденциальности

Практическая работа №9 Обеспечение безопасности локальной сети. Настройка параметров безопасности браузера

Цель: изучить возможности настройки безопасности локальной сети и браузера

Вопросы по практической работе:

1. Какие уязвимости ОС Windows были устранены в данной практической работе и какими путями?

2. Для чего используется утилита Netstat?

3. Перечислите, какие утилиты вошли в состав программы NetStat Agent? Для чего используется каждая из утилит?

4. Для чего используется программа Nmap? TCPView?

Тестовые задания

Как называется умышленно искаженная информация?

+ Дезинформация

- Информативный поток

- Достоверная информация

- Перестает быть информацией

Как называется информация, к которой ограничен доступ?

+ Конфиденциальная

- Противозаконная

- Открытая

- Недоступная

Какими путями может быть получена информация?

+ проведением, покупкой и противоправным добыванием информации научных исследований

- захватом и взломом ПК информации научных исследований

- добыванием информации из внешних источников и скремблированием информации научных исследовании

- захватом и взломом защитной системы для информации научных исследований

Основной документ, на основе которого проводится политика информационной безопасности?

+ программа информационной безопасности

- регламент информационной безопасности

- политическая информационная безопасность

- Протекторат

В зависимости от формы представления информация может быть разделена на?

+ Речевую, документированную и телекоммуникационную

- Мысль, слово и речь

- цифровая, звуковая и тайная

- цифровая, звуковая

К каким процессам относят процессы сбора, обработки, накопления, хранения, поиска и распространения информации

+ Информационным процессам

- Мыслительным процессам

- Машинным процессам

- Микропроцессам

Что называют защитой информации?

+ Все ответы верны

- Называют деятельность по предотвращению утечки защищаемой информации

- Называют деятельность по предотвращению несанкционированных воздействий на защищаемую информацию

- Называют деятельность по предотвращению непреднамеренных воздействий на защищаемую информацию

Под непреднамеренным воздействием на защищаемую информацию понимают?

+ Воздействие на нее из-за ошибок пользователя, сбоя технических или программных средств и воздействие природных явлений

- Процесс ее преобразования, при котором содержание информации изменяется на ложную

- Возможности ее преобразования, при котором содержание информации изменяется на ложную информацию

- Не ограничения доступа в отдельные отрасли экономики или на конкретные производства

Функция защиты информационной системы, гарантирующая то, что доступ к информации, хранящейся в системе может быть осуществлен только тем лицам, которые на это имеют право

- управление доступом
+ конфиденциальность
- аутентичность
- целостность
- доступность

Основные предметные направления Защиты Информации?

+ охрана государственной, коммерческой, служебной, банковской тайн, персональных данных и интеллектуальной собственности
- Охрана золотого фонда страны
- Определение ценности информации
- Усовершенствование скорости передачи информации

Государственная тайна это

+ защищаемые государством сведения в области его военной, внешнеполитической, экономической, разведывательной, контрразведывательной и оперативно-розыскной деятельности, распространение которых может нанести ущерб безопасности страны
- ограничения доступа в отдельные отрасли экономики или на конкретные производства
- защищаемые банками и иными кредитными организациями сведения о банковских операциях
- защищаемая по закону информация, доверенная или ставшая известной лицу (держателю) исключительно в силу исполнения им своих профессиональных обязанностей

Меры по защите информации от неавторизованного доступа, разрушения, модификации, раскрытия и задержек в доступе

+ Информационная безопасность
- Защитные технологии
- Заземление
- Конфиденциальность

Можно выделить следующие направления мер информационной безопасности

- Правовые
- Организационные
+ Все ответы верны
- Технические

Что можно отнести к правовым мерам ИБ?

+ Разработку норм, устанавливающих ответственность за компьютерные преступления, защиту авторских прав программистов, совершенствование уголовного и гражданского законодательства, а также судопроизводства
- охрану вычислительного центра, тщательный подбор персонала, исключение случаев ведения особо важных работ только одним человеком, наличие плана восстановления работоспособности центра и т.д.
- Защиту от несанкционированного доступа к системе, резервирование особо важных компьютерных подсистем, организацию вычислительных сетей с возможностью перераспределения ресурсов в случае нарушения работоспособности отдельных звеньев, установку оборудования обнаружения и тушения пожара, оборудования обнаружения воды, принятие конструкционных мер защиты от хищений, саботажа, диверсий, взрывов, установку резервных систем электропитания, оснащение помещений замками, установку сигнализации и многое другое
- охрану вычислительного центра, установку сигнализации и многое другое

Что можно отнести к организационным мерам ИБ?

- Разработку норм, устанавливающих ответственность за компьютерные преступления, защиту авторских прав программистов, совершенствование уголовного и гражданского законодательства, а также судопроизводства.

+ Охрану вычислительного центра, тщательный подбор персонала, исключение случаев ведения особо важных работ только одним человеком, наличие плана восстановления работоспособности центра и т.д.

- Защиту от несанкционированного доступа к системе, резервирование особо важных компьютерных подсистем.

- Охрану работоспособности отдельных звеньев и организацию вычислительных сетей с возможностью перераспределения ресурсов.

- Принятие конструкционных мер защиты от хищений, саботажа, диверсий, взрывов, установку резервных систем электропитания, оснащение помещений замками, установку сигнализации и многое другое.

Что можно отнести к техническим мерам ИБ?

- Разработку норм, устанавливающих ответственность за компьютерные преступления, защиту авторских прав программистов, совершенствование уголовного и гражданского законодательства, а также судопроизводства

- Охрану вычислительного центра, тщательный подбор персонала, исключение случаев ведения особо важных работ только одним человеком, наличие плана восстановления работоспособности центра и т.д.

+ Защиту от несанкционированного доступа к системе, резервирование особо важных компьютерных подсистем, организацию вычислительных сетей с возможностью перераспределения ресурсов в случае нарушения работоспособности отдельных звеньев и многое другое

- Простые и доступные меры защиты от хищений, саботажа, диверсий, взрывов

- В административных местах установку резервных систем электропитания, оснащение помещений замками, установку сигнализации и многое другое.

Обеспечение достоверности и полноты информации и методов ее обработки.

- Конфиденциальность

+ Целостность

- Доступность

- Целесообразность

Обеспечение доступа к информации только авторизованным пользователям?

+ Конфиденциальность

- Целостность

- Доступность

- Целесообразность

Целью информационной безопасности является?

+ все перечисленное

- обезопасить ценности системы

- защитить и гарантировать точность и целостность информации

- минимизировать разрушения

Укажите направления мер информационной безопасности.

+правовые, организационные, технические

-правовые, аппаратные, программные

-личные, организационные

-технические

Что такое Информационная безопасность?

+ меры по защите информации от неавторизованного доступа

-меры по защите ПК

-безопасность личной информации

-все перечисленное

Что такое компьютерный вирус?

Прикладная программа. Системная программа.

+Программа, выполняющая на компьютере несанкционированные действия. База данных.

Основные типы компьютерных вирусов: Аппаратные, программные, загрузочные. Программные, загрузочные, макровирусы.

+ Файловые, программные, макровирусы. **Этапы действия программного вируса:**

Размножение, вирусная атака.

Запись в файл, размножение.

+ Запись в файл, размножение, уничтожение программы.

В чем заключается размножение программного вируса?

Программа-вирус один раз копируется в теле другой программы.

+ Вирусный код неоднократно копируется в теле другой программы.

Что называется вирусной атакой?

Неоднократное копирование кода вируса в код программы.

Отключение компьютера в результате попадания вируса.

+ Нарушение работы программы, уничтожение данных, форматирование жесткого диска.

Какие существуют методы реализации антивирусной защиты?

Аппаратные и программные.

+ Программные и административные. Только программные.

Какие существуют основные средства защиты данных?

+ Резервное копирование наиболее ценных данных. Аппаратные средства.

Программные средства.

Какие существуют вспомогательные средства защиты?

Аппаратные средства.

Программные средства.

+ Административные методы и антивирусные программы.

На чем основано действие антивирусной программы?

На ожидании начала вирусной атаки.

+ На сравнении программных кодов с известными вирусами. На удалении зараженных файлов.

О каком вирусе идет речь?

«Могут привести к сбою и зависанию при работе компьютера»

Файловый

+ Опасный

Загрузочный

Этапы действия программного вируса:

Размножение, вирусная атака

+ Запись в файл, размножение, уничтожение.

Запись в файл, размножение.

Какие программы относятся к антивирусным?

+ AVP, DrWeb, Norton AntiVirus.

MS-DOS, MS Word, AVP .

MS Word, MS Excel, Norton Commander .

Какие существуют вспомогательные средства защиты?

+ Административные методы и антивирусные программы. Аппаратные средства.

Программные средства.

В чем заключается размножение программного вируса?

Программа-вирус один раз копируется в теле другой программы.

+ Вирусный код неоднократно копируется в теле другой программы.

Ответьте на вопрос «Что называется вирусной атакой?»

нарушение работы программы

уничтожение данных

форматирование жесткого диска.

Ответьте на вопрос «Какие существуют методы реализации антивирусной защиты?»

Программные и административные

На чем основано действие антивирусной программы?

На ожидании начала вирусной атаки

+ На сравнении программных кодов с известными вирусами

На удалении зараженных файлов

Какие существуют основные средства защиты данных?

Аппаратные средства

Программные средства

+Резервное копирование наиболее ценных данных

Меры по защите информации от неавторизованного доступа называется

+Информационной безопасностью

-Безопасностью ПК

-Личной безопасностью

- Безопасностью группы администратора

Средства аппаратной защиты, включающие средства защиты кабельной системы, систем электропитания относится к?

+техническим мерам защиты

- не правовым мерам защиты

-организационным мерам защиты

-программным средствам защиты

Защита от сбоев серверов, рабочих станций и локальных компьютеров относится к?

+аппаратным средствам защиты

-программным средствам защиты

-техническим средствам защиты

-правовым средствам защиты

Защищаемые программы для ПК находятся в?

+ ОЗУ и ЖМД

- ПЗУ и МГД

- МГД и Оп

- ПК и НГМД

К правовым мерам следует отнести?

+ разработку норм, устанавливающих ответственность за компьютерные преступления и защиту авторских прав программистов

-охрану вычислительного центра и аппаратуры связи

- проектирование ЛВС и ГБС

- средства идентификации и аутентификации пользователей

Потеря или изменение данных при ошибках ПО относится к

+ техническим и правовым мерам защиты

-организационным мерам защиты

- правовым мерам защиты

- мерам защиты от НДС и кражи

- к средствам идентификации и аутентификации

Защита от сбоев серверов, рабочих станций и локальных компьютеров относится к?

+Аппаратным и техническим средствам защиты

-Программным средствам защиты

-Средствам защиты идентификации и аутентификации

- Организационным и общим средствам защиты

Какой способ защиты информации присваивает значение каждому пользователю соответствующие права доступа к каждому ресурсу

+Права группы

-Аудит

-Шифрование данных

-Модели защиты

Методы сохранение данных при чрезвычайных ситуаций

-резервное копирование на магнитную ленту;

-источники бесперебойного питания (UPS);

-отказоустойчивые системы

+Все ответы верны

Какой способ данные, дублируя и размещая их на различных физических носителях (например, на разных дисках).

-Журнал резервного копирования

+Отказоустойчивые системы

-Метод резервного копирования

-Шифрование данных

Наиболее надежным средством предотвращения потерь информации при кратковременном отключении электроэнергии?

+ установка источников бесперебойного питания (UPS)

- Такого средства не существует

- Каждую минуту сохранять данные

- Перекидывать информацию на носитель, который не зависит от энергии

Средства защиты данных, функционирующие в составе программного обеспечения.

+ Программные средства защиты информации

- Технические средства защиты информации

- Источники бесперебойного питания (UPS)

- Смешанные средства защиты информации

Средством предотвращения потерь информации при кратковременном отключении электроэнергии является?

+источник бесперебойного питания (UPS)

-источник питания

-электро-переключатель

-все перечисленное

Технические меры защиты можно разделить на:

+ средства аппаратной защиты, включающие средства защиты кабельной системы, систем электропитания, и тд

-правовые, организационные, технические

-правовые, аппаратные, программные

-личные, организационные

Программные средства защиты можно разделить на:

+криптография, антивирусные программы, системы разграничения полномочий, средства контроля доступа и тд

- административные меры защиты, включающие подготовку и обучение персонала, организацию тестирования и приема в эксплуатацию программ,

контроль доступа в помещения и тд

-правовые, организационные, технические

-правовые, аппаратные, программные

К наиболее важному элементу аппаратной защиты можно отнести?

+ защита от сбоев серверов, рабочих станций и локальных компьютеров

-защиту от вирусов

-защиту от хакеров

-все перечисленное

Наибольшую угрозу для безопасности сети представляют.

+несанкционированный доступ, электронное подслушивание и преднамеренное или неумышленное повреждение

- вскрытие стандартной учётной записи пользователя

- вскрытие стандартной учётной группы администратора

- копирование файлов, которые были изменены в течение дня, без отметки о резервном копировании

Защита через права доступа заключается.

+присвоении каждому пользователю определенного набора прав

-запереть серверы в специальном помещении с ограниченным доступом

-присвоить пароль каждому общедоступному ресурсу

- в наличии преобразователя микрофона

Дифференцированное резервное копирование это

-Копирование только тех файлов, которые были изменены в течение дня, без отметки о резервном копировании

-Копирование всех выбранных файлов без отметки о резервном копировании

-Копирование и маркировка выбранных файлов, только если они были изменены со времени последнего копирования

+Копирование выбранных файлов, только если они были изменены со времени последнего резервного копирования, без отметки о резервном копировании

Disk mirroring – это

+дублирование раздела и запись его копии на другом физическом диске

-это пара зеркальных дисков, каждым из которых управляет отдельный контроллер

-При записи данных делится на части и распределяется по серверу

- Копирование только тех файлов, которые были изменены в течение дня, без отметки о резервном копировании

Как называются компьютерные системы, в которых обеспечивается безопасность информации?

+ защищенные КС

- небезопасные КС

- Само достаточные КС

- Саморегулирующиеся КС

Элемент аппаратной защиты, где используется резервирование особо важных компьютерных подсистем

- защита от сбоев в электропитании

+ защита от сбоев серверов, рабочих станций и локальных компьютеров

- защита от сбоев устройств для хранения информации

- защита от утечек информации электромагнитных излучений

Элемент аппаратной защиты, где используется организация надежной и эффективной системы резервного копирования и дублирования данных

- защита от сбоев в электропитании

- защита от сбоев серверов, рабочих станций и локальных компьютеров

+ защита от сбоев устройств для хранения информации

- защита от утечек информации электромагнитных излучений

Элемент аппаратной защиты, где используется экранирование, фильтрацию, заземление, электромагнитное зашумление, а также средства ослабления уровней нежелательных электромагнитных излучений.

- защита от сбоев в электропитании
- защита от сбоев серверов, рабочих станций и локальных компьютеров
- защита от сбоев устройств для хранения информации
+ защита от утечек информации электромагнитных излучений

Какая из перечисленных атак на поток информации является пассивной:+ перехват.

- имитация.
- модификация.
- фальсификация.
- прерывание.

Технические каналы утечки информации делятся на…

+ Все перечисленное
- Акустические и виброакустические
- Электрические
- Оптические

Какой технический канал утечки отвечает за распространение звуковых колебаний в любом звукопроводящем материале или среде?

+ Акустические и виброакустические
- Электрические
- Оптические
- Радиоканалы

Какой технический канал утечки отвечает за напряжение и токи в различных токопроводящих коммуникациях?

- Акустические и виброакустические
+ Электрические
- Оптические
- Радиоканалы

Какой технический канал утечки отвечает за электромагнитные излучения радиодиапазона?

- Акустические и виброакустические
- Электрические
- Оптические
+ Радиоканалы

Какой технический канал утечки отвечает за электромагнитные излучения в видимой, инфракрасной и ультрафиолетовой частях спектра?

- Акустические и виброакустические
- Электрические
+ Оптические
- Радиоканалы

Учет всех возможных коммуникационных каналов, обеспечения физической безопасности, шифрования резервных копий и информации, покидающей корпоративный периметр, и других организационных мероприятий это?

- Индивидуальный подход к защите
+ Комплексный подход к защите
- Смешанный подход к защите
- Рациональный подход к защите информация удаляется

Потенциальные угрозы, против которых направлены технические меры защиты информации

+ Потери информации из-за сбоев оборудования, некорректной работы программ и ошибки обслуживающего персонала и пользователей

- Потери информации из-за халатности обслуживающего персонала и не ведения системы наблюдения

- Потери информации из-за не достаточной установки резервных систем электропитании и оснащение помещений замками.

- Потери информации из-за не достаточной установки сигнализации в помещении.

- Процессы преобразования, при котором

Криптографические средства относится к?

+Программным средствам

-Аппаратным средствам

-Организационным средствам защиты

-Захвату данных

Шифрование информации это

+ Процесс ее преобразования, при котором содержание информации

становится непонятным для не обладающих соответствующими полномочиями субъектов

- Процесс преобразования, при котором информация удаляется

- Процесс ее преобразования, при котором содержание информации изменяется на ложную

- Процесс преобразования информации в машинный код

Программные средства защиты информации.

+ средства архивации данных, антивирусные программы

- Технические средства защиты информации

- Источники бесперебойного питания (UPS)

- Смешанные средства защиты информации

Программное средство защиты информации.

+ криптография

- источник бесперебойного питания

- резервное копирование

- дублирование данных

Запуск утилиты Setup выполняется нажатием кнопки?

+Delete

-Alt

-Tab

-F2

Чтобы установить парольную защиту в ОС Windows , необходимо выполнить следующую процедуру?

+Пуск->Панель управления->Учетные записи->Изменение пароля

-Пуск->Учетные записи->Изменение пароля

-Пуск->Справка->Учетные записи->Изменение пароля

-Пуск->Панель управления->Пароли и данные->Изменение пароля

При вводе пароля с клавиатуры его длина может достигать до?

+64 символов

-128 символов

-32 символов

-512 символов

Служат обеспечению сохранения целостности программного обеспечения в составе вычислительной системы

+пароль

-корпус вычислительной системы

-шифры

-сигналы

В каких случаях криптография неэффективна?

+ когда элементы текста известны в зашифрованном и исходном виде

- когда элементы текста известны в открытом и активном виде

- если есть пароль и логин

- когда элементы текста представлены в открытом и не полном виде

В каком случае надежнее шифр?

+короткий зашифрованный текст

-длинный зашифрованный текст

-зашифрованный текст среднего размера

-зашифрованный текст не влияет на надежность шифра

Как связаны ключи шифрования между собой?

+математической функцией

-связкой

-шифром

-специальным паролем

В каких случаях возможно вычисление одного ключа с помощью другого

+ Использованием только ЭВМ

- Ни в каких случаях невозможна

- Использованием математической функцией

- Использованием только ЛВС

Назначение пароля в ИС?

+ механизм управления доступом, средство защиты и безопасность личной информации

- скрытие копирования участков магнитной ленты из ОЗУ в ПЗУ

- технические меры защиты и средство защиты данных

- участки магнитной ленты скрытые шифром

- механизм управления средствами защиты и безопасность доступа к ОЗУ в ПЗУ

Меры по защите информации от неавторизованного доступа называется

+Информационной безопасностью

-Безопасностью ПК

-Личной безопасностью

-Средства защиты

-Меры скрытия копирования

Средства аппаратной защиты, включающие средства защиты кабельной системы, систем электропитания относится к?

+ техническим мерам защиты и правовым мерам защиты

-организационным мерам защиты

- меры скрытия копирования участков магнитной ленты из ОЗУ в ПЗУ

Защита от сбоев серверов, рабочих станций и локальных компьютеров относится к?

+аппаратным средствам защиты

-программным средствам защиты

-техническим средствам защиты

-правовым средствам защиты

Самый известный в России производитель систем защиты от вирусов, спама и хакерских атак.

+лаборатория Касперского

-Российский центр по защите от вредоносных программ

-компания McAfee Security

-лаборатория доктора Веб

-компания Тумар

Один из механизмов защиты использующих в сети для обеспечения конфиденциальности

+управление маршрутизацией

-генерация трафика

-защитный канал

-защитный механизм

-генерация данных

Развитие современных средств безбумажного документооборота, средств электронных платежей немыслимо без развития средств доказательства подлинности и целостности документа. Таким средством является

+ электронно-цифровая подпись

-протокол секретности

-аутентификация

-биометрия

-идентификация пользователя

-водяные знаки

При генерации электронно – цифровой подписи используются…

+общие параметры, секретный ключ и открытый ключ

-открытый ключ, закрытый ключ

-общие параметры, секретный ключ и закрытый ключ

-общие параметры, секретный ключ и конверт защиты

-один секретный ключ

Информация основной объект защиты, ее сохранность и конфиденциальность это основа

+информационной безопасности -информационной защищенности

-объективность защищенности

-информатики и компьютерных сетей

При каком случае срабатывает сигнал самоуничтожения программы

+при несанкционированном копировании программы из ПЗУ в ОЗУ

-при несанкционированном копировании программы из ОЗУ в ПЗУ

- при непредвиденном включении преобразователя микрофона

-при непредвиденном отключении ПК

Что такое пароль?

+механизм управления доступом

-средство защиты

-безопасность личной информации

- Безопасность людей

Как связаны ключи шифрования между собой?

+математической функцией

-связкой

-шифром

-специальным паролем

Наиболее распространенный криптографический код

+Код Хэмминга

-код Рида-Соломона

-код Морзе

-итеративный код.

10.2 Критерии оценки результатов текущего контроля освоения дисциплины

Критерии оценки ответов на контрольные вопросы

Оценка, уровень достижения компетенций	Описание критериев
Отлично, высокий	Обучающийся демонстрирует уверенное знание материала, полно излагает материал, дает правильное определение основных понятий; обнаруживает понимание материала, может обосновать свои суждения, применить знания на практике, привести необходимые примеры не только из учебника, но и самостоятельно составленные; излагает материал последовательно и правильно с точки зрения норм литературного языка
Хорошо, продвинутый	Обучающийся демонстрирует уверенное знание материала, но допускает 1–2 ошибки, которые сам же исправляет, и 1–2 недочета в последовательности и языковом оформлении излагаемого.
Удовлетворительно, пороговый	Обучающийся обнаруживает знание и понимание основных положений данной темы, но излагает материал неполно и допускает неточности в определении понятий или формулировке правил; не умеет достаточно глубоко и доказательно обосновать свои суждения и привести свои примеры; излагает материал непоследовательно и допускает ошибки в языковом оформлении излагаемого.
Неудовлетворительно, компетенция не освоена	Обучающийся демонстрирует незнание большей части соответствующего вопроса, допускает ошибки в формулировке определений и правил, искажающие их смысл, беспорядочно и неуверенно излагает материал.

Критерии оценки практической работы

Оценка «отлично» – ставиться, если обучающийся демонстрирует знание теоретического и практического материала по теме практической работы, определяет взаимосвязи между показателями задачи, даёт правильный алгоритм решения, определяет междисциплинарные связи по условию задания. А также, если обучающийся имеет глубокие знания учебного материала по теме практической работы, показывает усвоение взаимосвязи основных понятий используемых в работе, смог ответить на все уточняющие и дополнительные вопросы.

Оценка «хорошо» – ставится, если обучающийся демонстрирует знание теоретического и практического материала по теме практической работы, допуская незначительные неточности при решении задач, имея неполное понимание междисциплинарных связей при правильном выборе алгоритма решения задания. А также, если обучающийся показал знание учебного материала, усвоил основную литературу, смог ответить почти полно на все заданные дополнительные и уточняющие вопросы.

Оценка «удовлетворительно» – ставится, если обучающийся затрудняется с правильной оценкой предложенной задачи, дает неполный ответ, требующий наводящих вопросов преподавателя, выбор алгоритма решения задачи возможен при наводящих вопросах преподавателя. А также, если обучающийся в целом освоил материал практической работы, ответил не на все уточняющие и дополнительные вопросы.

Оценка «неудовлетворительно» – ставится, если обучающийся дает неверную оценку ситуации, неправильно выбирает алгоритм действий. А также, если он имеет существенные пробелы в знаниях основного учебного материала практической работы, ко-

торый полностью не раскрыл содержание вопросов, не смог ответить на уточняющие и дополнительные вопросы.

Критерии оценки тестовых заданий

Оценка, уровень достижения компетенций	Описание критериев
Отлично, высокий	Содержание правильных ответов в тесте не менее 90%
Хорошо, продвинутый	Содержание правильных ответов в тесте не менее 75%
Удовлетворительно, пороговый	Содержание правильных ответов в тесте не менее 50%
Неудовлетворительно, компетенция не освоена	Содержание правильных ответов в тесте менее 50%

10.3. Оценочные материалы для промежуточной аттестации по дисциплине

Вопросы для проведения зачета

1. Понятие национальной безопасности Российской Федерации.
2. Национальные интересы РФ и стратегические национальные приоритеты.
3. Роль информационной безопасности в обеспечении национальной безопасности государства.
4. Основные составляющие национальных интересов Российской Федерации в информационной сфере.
5. Понятие информационной безопасности Российской Федерации.
6. Интересы личности общества и государства в информационной сфере.
7. Виды угроз информационной безопасности Российской Федерации.
8. Внешние и внутренние источники угроз информационной безопасности Российской Федерации.
9. Методы обеспечения информационной безопасности Российской Федерации
10. Источники понятий в области информационной безопасности.
11. Основные понятия информационной безопасности.
12. Общеметодологические принципы теории информационной безопасности.
13. Понятие и сущность защищаемой информации.
14. Права и обязанности обладателя информации.
15. Виды защищаемой информации.
16. Перечень сведений конфиденциального характера.
17. Понятие интеллектуальной собственности и особенности ее защиты.
18. Понятие угрозы информационной безопасности.
19. Фактор, воздействующий на защищаемую информацию. Типы дестабилизирующих факторов.
20. Классификация и виды угроз информационной безопасности.
21. Внутренние и внешние источники угроз информационной безопасности.
22. Угрозы утечки информации и угрозы несанкционированного доступа.
23. Основные элементы канала реализации угрозы безопасности информации.
24. Субъекты и цели информационного противоборства.
25. Составные части и методы информационного противоборства.
26. Информационное оружие, его классификация и возможности.
27. Методы нарушения конфиденциальности, целостности и доступности информации.
28. Информационная война как способ воздействия на информационные системы.
29. Информационная безопасность критически важных объектов.

30. Обеспечение безопасности объектов информационной сферы государства в информационной войне.

31. Компьютерная система как объект информационной безопасности.

32. Основные способы защиты информации.

33. Понятие и классификация средств защиты информации.

34. Характеристика средств защиты информации.

35. Уровни информационной безопасности и их характеристика.

36. Сервисы безопасности программно-технического уровня.

37. Идентификация и аутентификация как сервисы безопасности.

38. Управление доступом и его виды.

39. Авторизация как сервис безопасности.

40. Протоколирование и аудит как сервисы безопасности.

41. Криптографические сервисы безопасности.

42. Экранирование как сервис безопасности.

43. Анализ защищенности как сервис безопасности.

44. Туннелирование как сервис безопасности.

45. Управление как сервис безопасности.

46. Назначение формальных моделей безопасности. Политика безопасности.

47. Дискреционная модель безопасности. Модель Харрисона-Руззо-Ульмана.

48. Мандатная модель безопасности. Модель Белла-ЛаПадулы.

49. Формальные модели целостности.

50. Понятие ролевого управления доступом.

51. Модели, стратегии и системы обеспечения информационной безопасности.

52. Критерии безопасности компьютерных систем «Оранжевая книга».

53. Общие критерии безопасности информационных технологий.

54. Критерии и классы защищенности СВТ и АС. Руководящие документы ФСТЭК России.

55. Стандарты по управлению информационной безопасностью ISO/IEC 27000.

56. Классификация и возможности технических разведок.

57. Компьютерная разведка.

58. Технические каналы утечки информации при эксплуатации автоматизированных систем.

59. Электромагнитное воздействие и эффекты его воздействия.

60. Защита автоматизированных систем и средств вычислительной техники от внешнего электромагнитного воздействия.

10.4 Показатели, критерии и шкала оценивания ответов на зачете

Оценка, уровень достижения компетенций	Описание критериев
Зачтено, высокий	Обучающийся выполнил все задания, предусмотренные рабочей программой, отчитался об их выполнении, демонстрируя отличное знание освоенного материала и умение самостоятельно решать сложные задачи дисциплины
Зачтено, продвинутый	Обучающийся выполнил все задания, предусмотренные рабочей программой, отчитался об их выполнении, демонстрируя хорошее знание освоенного материала и умение самостоятельно решать стандартные задачи дисциплины

Зачтено, пороговый	Обучающийся выполнил все задания, предусмотренные рабочей программой, отчитался об их выполнении, демонстрируя знание основ освоенного материала и умение решать стандартные задачи дисциплины с помощью преподавателя
Не зачтено, компетенция не освоена	Обучающийся выполнил не все задания, предусмотренные рабочей программой или не отчитался об их выполнении, не подтверждает знание освоенного материала и не умеет решать стандартные задачи дисциплины даже с помощью преподавателя