МИНОБРНАУКИ РОССИИ
Ярославский государственный университет им. П.Г. Демидова

Кафедра компьютерной безопасности и математических методов обработки информации

УТВЕРЖДАЮ
Декан математического факультета
_____П.Н. Нестеров
(подпись)
«19» апреля 2022 г.

Рабочая программа дисциплины
«Безопасность в современной информационной среде»

Направление подготовки
38.03.02 **Менеджмент**

Направленность (профиль)
«**Управление проектами**»

Форма обучения
Очная

Программа одобрена
на заседании кафедры
от 11.05.2022 года, протокол № 8

Программа одобрена НМК
математического факультета
протокол № 5 от 11.05.2022 года

Ярославль
2022

1. Цели освоения дисциплины

Дисциплина «Безопасность в современной информационной среде» обеспечивает приобретение обучающимися знаний, умений и навыков по компетенции ОПК-1. «Способен понимать принципы работы современных информационных технологий и использовать их для решения задач профессиональной деятельности» Федерального государственного образовательного стандарта высшего образования по направлению подготовки 39.03.01 Социология.

Основной целью изучения дисциплины является теоретическая и практическая подготовка обучающихся к деятельности, связанной с применением современных средств и методов защиты информации в повседневной и профессиональной деятельности. Курс дает представление о месте и роли информационной безопасности в современном мире. Его изучение дает возможность сознательного использования, обработки и защиты информации.

2. Место дисциплины в структуре образовательной программы

Данная дисциплина относится к обязательной части образовательной программы.

Дисциплина «Безопасность в современной информационной среде» играет важную роль для общепрофессиональной подготовки обучающегося.

3. Планируемые результаты обучения по дисциплине, соотнесенные с планируемыми результатами освоения ОП бакалавриата

Процесс изучения дисциплины направлен на формирование следующих компетенций в соответствии с ФГОС ВО, ООП ВО и приобретения следующих знаний, умений, навыков и (или) опыта деятельности:

Формируемая компетенция (код и формулировка)	**Индикатор достижения компетенции (код и формулировка)**	**Перечень планируемых результатов обучения**
Общепрофессиональные компетенции		
ОПК-5. Способен использовать современные информационные технологии и программные средства при решении профессиональных задач	**ОПК-5.1**. Использует современные информационные технологии и программные средства при решении профессиональных задач.	*Знать:* основные понятия в области обработки и защиты информации и их определения; последовательность выполнения работ по защите информации; классификацию нарушителей информационной безопасности; виды и назначение средств защиты информации. *Уметь:* устанавливать и осуществлять первичную настройку операционных систем, антивирусных средств и межсетевых экранов. *Владеть навыками:* работы со средствами защиты информации
	ОПК-5.2. Решает стандартные задачи профессиональной	*Знать:* Основные принципы административно-правовой защиты информации;

	деятельности на основе информационных технологий с учетом основных требований информационной безопасности.	*Уметь:* реагировать на различные угрозы информационной безопасности и применять современные технологии для ее обеспечения; *владеть навыками:* применения, антивирусных систем и систем распознавания угроз и атак.

4. Объем, структура и содержание дисциплины

Общая трудоемкость дисциплины составляет 2 зачетные единицы, 72 акад. часа.

Очная форма

№ п/п	**Темы (разделы) дисциплины, их содержание**	**Семестр**	**Виды учебных занятий, включая самостоятельную работу студентов, и их трудоемкость (в академических часах)**						**Формы текущего контроля успеваемости** **Форма промежуточной аттестации** ***(по семестрам)***
			Контактная работа						
			лекции	практические	лабораторные	консультации	аттестационные испытания	самостоятельная работа	
Раздел 1	**Правовые и организационные основы обеспечения информационной безопасности в Российской Федерации**	2	**6**					**3**	
Тема 1.1	Правовые основы обеспечения информационной безопасности	2	2					1	Тест
Тема 1.2	Защита персональных данных	2	2					1	Тест
Тема 1.3	Организационные основы обеспечения информационной безопасности	2	2					1	Тест
	в том числе с ЭО и ДОТ		6					**3**	Видеолекции текстовые материалы

									учебного пособия, презентации, тест в ЭУК в DemidOnline
Раздел 2	**Архитектура компьютера**	2	**2**					**1**	
Тема 2.1	Архитектура компьютера	2	2					1	Тест
	в том числе с ЭО и ДОТ		2					1	Видеолекции текстовые материалы учебного пособия, презентации, тест в ЭУК в DemidOnline
Раздел 3	**Основы информационной безопасности в операционных системах**	2	**3**	**7**				**9**	Тест
Тема 3.1	Введение в информационную безопасность операционных систем	2	1	2				3	Тест
Тема 3.2	Информационная безопасность операционных систем семейства Windows	2	1	2				3	Тест
Тема 3.3	Информационная безопасность операционных систем семейства Linux	2	1	3				3	Тест
	в том числе с ЭО и ДОТ		3	3				9	Видеолекции текстовые материалы учебного пособия, презентации, тест в ЭУК в DemidOnline
Раздел 4	**Основы информационной безопасности в локальных вычислительных сетях**	2	**3**	**7**				**9**	
Тема 4.1	Введение в архитектуру локальных вычислительных	2	1	2				4	Тест

	сетей								
Тема 4.2	Сетевые угрозы и методы противодействия им	2	1	2				4	Тест
Тема 4.3	Межсетевые экраны	2	1	3				3	Тест
	в том числе с ЭО и ДОТ		3	3				11	Видеолекции текстовые материалы учебного пособия, презентации, тест в ЭУК в DemidOnline
Раздел 5	**Криптографические методы защиты информации**	2	**2**	**2**				**3**	
Тема 5.1	Введение в криптографические методы защиты информации	2	2	2				3	Тест
	в том числе с ЭО и ДОТ		2	1				3	Видеолекции текстовые материалы учебного пособия, презентации, тест в ЭУК в DemidOnline
		2					0,3	10,7	Зачет
	Всего за 2 семестр	72	16	16			0,3	37,7	
	Всего	**72**	**16**	**16**		**2**	**0,3**	**37,7**	

Очно-заочная форма

№ п/п	**Темы (разделы) дисциплины, их содержание**	**Семестр**	**Виды учебных занятий, включая самостоятельную работу студентов, и их трудоемкость (в академических часах)**						**Формы текущего контроля успеваемости** **Форма промежуточной аттестации** ***(по семестрам)***
			Контактная работа						
			лекции	практические	лабораторные	консультации	аттестационные испытания	самостоятельная работа	
Раздел 1	**Правовые и организационные основы обеспечения**	2	**6**					**3**	

	информационной безопасности в Российской Федерации								
Тема 1.1	Правовые основы обеспечения информационной безопасности	2	2					1	Тест
Тема 1.2	Защита персональных данных	2	2					1	Тест
Тема 1.3	Организационные основы обеспечения информационной безопасности	2	2					1	Тест
	в том числе с ЭО и ДОТ		6					**3**	Видеолекции текстовые материалы учебного пособия, презентации, тест в ЭУК в DemidOnline
Раздел 2	**Архитектура компьютера**	2	**2**					**1**	
Тема 2.1	Архитектура компьютера	2	2					1	Тест
	в том числе с ЭО и ДОТ		2					1	Видеолекции текстовые материалы учебного пособия, презентации, тест в ЭУК в DemidOnline
Раздел 3	**Основы информационной безопасности в операционных системах**	2	**3**	**7**				**9**	Тест
Тема 3.1	Введение в информационную безопасность операционных систем	2	1	2				3	Тест
Тема 3.2	Информационная безопасность операционных систем семейства Windows	2	1	2				3	Тест
Тема 3.3	Информационная безопасность операционных систем семейства	2	1	3				3	Тест

	Linux								
	в том числе с ЭО и ДОТ		3	3				9	Видеолекции текстовые материалы учебного пособия, презентации, тест в ЭУК в DemidOnline
Раздел 4	**Основы информационной безопасности в локальных вычислительных сетях**	2	**3**	**7**				**9**	
Тема 4.1	Введение в архитектуру локальных вычислительных сетей	2	1	2				4	Тест
Тема 4.2	Сетевые угрозы и методы противодействия им	2	1	2				4	Тест
Тема 4.3	Межсетевые экраны	2	1	3				3	Тест
	в том числе с ЭО и ДОТ		3	3				11	Видеолекции текстовые материалы учебного пособия, презентации, тест в ЭУК в DemidOnline
Раздел 5	**Криптографические методы защиты информации**	2	**2**	**2**				**3**	
Тема 5.1	Введение в криптографические методы защиты информации	2	2	2				3	Тест
	в том числе с ЭО и ДОТ		2	1				3	Видеолекции текстовые материалы учебного пособия, презентации, тест в ЭУК в DemidOnline
		2					0,3	10,7	Зачет
	Всего за 2 семестр	72	16	16			0,3	37,7	
	Всего	**72**	**16**	**16**		**2**	**0,3**	**37,7**	

Содержание разделов программы дисциплины
«Безопасность современной информационной среде»

Раздел 1. Правовые и организационные основы обеспечения информационной безопасности в Российской Федерации.

Тема 1.1. Правовые основы обеспечения информационной безопасности.

Основные права граждан в сфере обработки и защиты информации. Основные принципы правового регулирования в области обработки и защиты информации. Информация. Основные свойства безопасности информации: конфиденциальность, целостность, доступность. Виды информации по порядку доступа и распространения. Ограничение доступа к информации. Виды тайн. Обладатель информации. Информационные технологии. Информационные системы. Оператор информационной системы. Защита информации. Объекты защиты. Виды ответственности в сфере обработки и защиты информации.

Тема 1.2. Защита персональных данных.

Персональные данные и принципы их обработки. Виды персональных данных: специальные, биометрические и общедоступные. Условия обработки персональных данных. Согласие на обработку персональных данных. Трансграничная передача персональных данных. Права субъектов персональных данных. Оператор персональных данных и его обязанности. Меры обеспечения безопасности персональных данных. Контроль и надзор за выполнением мер по обеспечению безопасности. Уполномоченный орган по защите прав субъектов персональных данных.

Тема 1.3. Организационные основы обеспечения информационной безопасности.

Какие вопросы ставит информационная безопасность? Последовательность действий по защите информации. Выявление и анализ информационных активов. Формирование требований по защите информации. Подходы к моделированию нарушителей и угроз информационной безопасности. Выбор средств и методов защиты информации. Внедрение системы защиты информации. Эксплуатация системы защиты информации.

Раздел 2. Архитектура компьютера.

Тема 2.1. Введение в архитектуру компьютера.

Процессоры. Основная (кэш и оперативная) память. Вспомогательная память. Устройства ввода-вывода (шины, мониторы, клавиатуры и мыши, веб-камеры, принтеры). Персональные компьютеры и мобильные устройства.

Раздел 3. Основы информационной безопасности в операционных системах.

Тема 3.1. Введение в информационную безопасность операционных систем.

Общий способ хранения и обработки информации в компьютере. Понятия операционной и файловой систем. Субъекты, объекты, методы и права доступа, привилегии субъекта доступа. Дискреционное управление доступом, мандатное управление доступом. Идентификация, аутентификация и авторизация. Аутентификация на основе паролей, на основе внешних носителей ключа, биометрическая аутентификация.

Тема 3.2. Информационная безопасность операционных систем семейства Windows.

Управление доступом в операционных системах семейства Windows. Идентификация, аутентификация и авторизация в операционных системах семейства Windows. Реализация аудита в операционных системах семейства Windows.

Тема 3.3. Информационная безопасность операционных систем семейства Linux.

Управление доступом в операционных системах семейства Linux. Идентификация, аутентификация и авторизация в операционных системах семейства Linux. Реализация аудита в операционных системах семейства Linux.

Раздел 4. Основы информационной безопасности в локальных вычислительных сетях.

Тема 4.1. Введение в архитектуру локальных вычислительных сетей.

Локальные вычислительные сети. Модель ISO/OSI. Архитектура и основные протоколы локальных вычислительных сетей.

Тема 4.2. Сетевые угрозы и методы противодействия им.

Классификации сетевых угроз, уязвимостей и атак. Сетевые атаки на различных уровнях модели ISO/OSI. Классификация вредоносного программного обеспечения. Признаки присутствия вредоносного программного обеспечения. Методы обнаружения.

Тема 4.3. Межсетевые экраны.

Межсетевые экраны (МЭ). Место и роль МЭ в обеспечении сетевой безопасности. Классификация МЭ. Основные возможности МЭ. Достоинства и недостатки МЭ. Построение правил фильтрации.

Раздел 5. Криптографические методы защиты информации.

Тема 5.1. Введение в криптографические методы защиты информации.

Исторический очерк развития криптографии. Симметричная и асимметричная криптография. Вычислительно сложные задачи математики. Криптосистема RSA. Понятие криптографического протокола. Свойства протоколов, характеризующие их безопасность. Схемы цифровой подписи.

5. Образовательные технологии, в том числе технологии электронного обучения и дистанционные образовательные технологии, используемые при осуществлении образовательного процесса по дисциплине

В процессе обучения используются следующие образовательные технологии:

Академическая лекция (или лекция общего курса) – последовательное изложение материала, осуществляемое преимущественно в виде монолога преподавателя. Требования к академической лекции: современный научный уровень и насыщенная информативность, убедительная аргументация, доступная и понятная речь, четкая структура и логика, наличие ярких примеров, научных доказательств, обоснований, фактов.

Проблемная лекция – изложение материала, предполагающее постановку проблемных и дискуссионных вопросов, освещение различных научных подходов,

авторские комментарии, связанные с различными моделями интерпретации изучаемого материала. Проблемная лекция начинается с вопросов, с постановки проблемы, которую в ходе изложения материала необходимо решить. В лекции сочетаются проблемные и информационные начала. При этом процесс познания студентов в сотрудничестве и диалоге с преподавателем приближается к поисковой, исследовательской деятельности. Содержание проблемы раскрывается путем организации поиска ее решения или суммирования и анализа традиционных и современных точек зрения.

Практическое занятие – занятие, посвященное освоению конкретных умений и навыков и закреплению полученных на лекции знаний.

Электронный учебный курс «Безопасность в современной информационной среде» на платформе онлайн-обучения DemidOnline, в котором:

- представлены видео-лекций по всем темам дисциплины и презентации к ним;
- представлены тексты лекций по всем темам дисциплины;
- представлены правила прохождения промежуточной аттестации по дисциплине;
- представлены тесты по темам дисциплины для самостоятельной работы обучающихся;
- посредством форума осуществляется синхронное и (или) асинхронное взаимодействие между обучающимися и преподавателем в рамках изучения дисциплины.

6. Перечень лицензионного и (или) свободно распространяемого программного обеспечения, используемого при осуществлении образовательного процесса по дисциплине

В процессе осуществления образовательного процесса используются:

- программное обеспечение для создания и демонстрации презентаций, иллюстраций и других учебных материалов:
  - Microsoft Windows (в составе Microsoft Imagine Premium Electronic Software Delivery);
  - Microsoft OfficeSTD 2013;
  - Virtual Box (свободно распространяемое ПО);
  - Ubuntu (свободно распространяемое ПО);
  - Kali Linux (свободно распространяемое ПО).
- для поиска учебной литературы библиотеки ЯрГУ – Автоматизированная библиотечная информационная система «БУКИ-NEXT» (АБИС «Буки-Next»);
- при проведении лекций используются мультимедийные презентации;
- при проведении лабораторных работ используются средства вычислительной техники, поддерживающие перечисленное программное обеспечение.

7. Перечень современных профессиональных баз данных и информационных справочных систем, используемых при осуществлении образовательного процесса по дисциплине

1. Электронные каталоги НБ ЯрГУ

(http://www.lib.uniyar.ac.ru/opac/bk_cat_find.php) содержат библиографические записи всех видов документов, составляющих фонд библиотеки, на русском и иностранных языках.

2. Электронная библиотека учебных материалов ЯрГУ

(http://www.lib.uniyar.ac.ru/opac/bk_cat_find.php) содержит более 2500 полных текстов учебных и учебно-методических материалов по основным изучаемым

дисциплинам, изданных в университете. Доступ в сети университета, либо по логину/паролю.

3. Справочно-правовая система «Консультантплюс»

(https://www.consultant.ru/**)** справочно-правовая система по законодательству Российской Федерации.

4. Справочно-правовая система «Гарант»

(http://www.garant.ru/**)** справочно-правовая система по законодательству Российской Федерации.

8. Перечень основной и дополнительной учебной литературы, ресурсов информационно-телекоммуникационной сети «Интернет» (при необходимости), рекомендуемых для освоения дисциплины

а) основная литература

а) основная литература

1. Безопасность в современной информационной среде. Часть 1: учебное пособие. В.Н. Князев, Д.М. Мурин; Яросл. гос. ун-т им. П.Г. Демидова. - Ярославль: ИНДИГО, 2021. – 158 с. [https://e.lanbook.com/book/75150]
2. Догадин, Н. Б. Архитектура компьютера : учебное пособие / Н. Б. Догадин. — 4-е изд. — Москва : Лаборатория знаний, 2020. — 274 с.
3. Буза, М. К. Архитектура компьютеров : учебник / М. К. Буза. — Минск : Вышэйшая школа, 2015. — 414 с. [https://e.lanbook.com/book/75150]
4. Солоневич, А. В. Компьютерные сети : учебник / А. В. Солоневич. — Минск : РИПО, 2021. — 208 с. [https://e.lanbook.com/book/194950]
5. Ракитин, Р. Ю. Компьютерные сети : учебное пособие / Р. Ю. Ракитин, Е. В. Москаленко. — Барнаул : АлтГПУ, 2019. — 340 с. [https://e.lanbook.com/book/139182]
6. Коржик, В. И. Основы криптографии : учебное пособие / В. И. Коржик, В. А. Яковлев. — Санкт-Петербург : Интермедия, 2017. — 312 с. [https://e.lanbook.com/book/161359]

б) дополнительная литература

б) дополнительная литература

1. Конституция Российской Федерации: [принята всенародным голосованием 12.12.1993 с изменениями, одобренными в ходе общероссийского голосования 01.07.2020]. — Доступ из справочно-правовой системы «Консультантплюс». — Текст: электронный.
2. Уголовный кодекс Российской Федерации: Федеральный закон от 13.06.1996 №63-ФЗ: [принят Государственной Думой 24.05.1996]: (с изменениями и дополнениями). — Доступ из справочно-правовой системы «Консультантплюс». — Текст: электронный.
3. Кодекс Российской Федерации об административных правонарушениях: Федеральный закон от 30.12.2001 №195-ФЗ: [принят Государственной Думой 20.12.2001]: (с изменениями и дополнениями). — Доступ из справочно-правовой системы «Консультантплюс». —Текст: электронный.
4. Трудовой кодекс Российской Федерации: Федеральный закон от 30.12.2001 №197-ФЗ: [принят Государственной Думой 21.12.2001]: (с изменениями и

дополнениями). — Доступ из справочно-правовой системы «Консультантплюс». — Текст: электронный.
5. Федеральный закон от 27.07.2006 №149-ФЗ «Об информации, информационных технологиях и о защите информации»: [принят Государственной Думой 08.07.2006]: (с изменениями и дополнениями). — Доступ из справочно-правовой системы «Консультантплюс». —Текст: электронный.
6. Федеральный закон от 27.07.2006 №152-ФЗ «О персональных данных»: [принят Государственной Думой 08.07.2006]: (с изменениями и дополнениями). — Доступ из справочно-правовой системы «Консультантплюс». —Текст: электронный.
7. Положение о порядке обращения со служебной информацией ограниченного распространения в федеральных органах исполнительной власти, уполномоченном органе управления использованием атомной энергии и уполномоченном органе по космической деятельности»: [утверждено Постановлением Правительства Российской Федерации от 03.11.1994 №1233]: (с изменениями и дополнениями). — Доступ из справочно-правовой системы «Консультантплюс». —Текст: электронный.
8. Требования к защите персональных данных при их обработке в информационных системах персональных данных: [утверждены Постановлением Правительства Российской Федерации от 01.11.2012 №1119]. — Доступ из справочно-правовой системы «КонсультантпПлюс». —Текст: электронный.
9. Перечень мер, направленных на обеспечение выполнения обязанностей, предусмотренных Федеральным законом «О персональных данных» и принятыми в соответствии с ним нормативными правовыми актами, операторами, являющимися государственными или муниципальными органами: [утвержден Постановлением Правительства Российской Федерации от 21.03.2012 №211]: (с изменениями и дополнениями). — Доступ из справочно-правовой системы «КонсультантпПлюс». —Текст: электронный.
10. Положение об особенностях обработки персональных данных, осуществляемой без использования средств автоматизации: [утверждено Постановлением Правительства Российской Федерации от 15.09.2008 №687]. — Доступ из справочно-правовой системы «КонсультантпПлюс». —Текст: электронный.
11. Требования к материальным носителям биометрических персональных данных и технологиям хранения таких данных вне информационных систем персональных данных: [утверждено Постановлением Правительства Российской Федерации от 06.07.2008 №512]: (с изменениями и дополнениями). — Доступ из справочно-правовой системы «КонсультантпПлюс». —Текст: электронный.
12. Методические рекомендации по уведомлению уполномоченного органа о начале обработки персональных данных и о внесении изменений в ранее представленные сведения: [утверждены приказом Роскомнадзора от 30.05.2017 №94]: (с изменениями и дополнениями). — Доступ из справочно-правовой системы «КонсультантпПлюс». —Текст: электронный.
13. Требования и методы по обезличиванию персональных данных: [утверждены приказом Роскомнадзора от 05.09.2013 №996]. — Доступ из справочно-правовой системы «КонсультантпПлюс». —Текст: электронный.
14. Состав и содержание организационных и технических мер по обеспечению безопасности персональных данных при их обработке в информационных системах персональных данных: [утверждены приказом ФСТЭК России от 18.02.2013 №21]: (с изменениями и дополнениями). — Доступ из справочно-правовой системы «КонсультантпПлюс». —Текст: электронный.

15. Базовая модель угроз безопасности персональных данных при их обработке в информационных системах персональных данных (Выписка): [утверждена Заместителем директора ФСТЭК России 15.02.2008]. — Доступ из справочно-правовой системы «КонсультантпПлюс». —Текст: электронный.
16. Методика определения актуальных угроз безопасности персональных данных при их обработке в информационных системах персональных данных: [утверждена Заместителем директора ФСТЭК России 14.02.2008]. — Доступ из справочно-правовой системы «КонсультантпПлюс». —Текст: электронный.
17. Состав и содержание организационных и технических мер по обеспечению безопасности персональных данных при их обработке в информационных системах персональных данных с использованием средств криптографической защиты информации, необходимых для выполнения установленных Правительством Российской Федерации требований к защите персональных данных для каждого из уровней защищенности: [утверждены приказом ФСБ России от 10.07.2014 №378]. — Доступ из справочно-правовой системы «КонсультантпПлюс». —Текст: электронный.
18. Методические рекомендации по разработке нормативных правовых актов, определяющих угрозы безопасности персональных данных, актуальные при обработке персональных данных в информационных системах персональных данных, эксплуатируемых при осуществлении соответствующих видов деятельности: [утверждены руководством 8 Центра ФСБ России 31.03.2015 №149/7/2/6-432]. — Доступ из справочно-правовой системы «КонсультантпПлюс». —Текст: электронный.
19. ГОСТ Р 51275-2006 Защита информации. Объект информатизации. Факторы, воздействующие на информацию. Общие положения. — Доступ из справочно-правовой системы «ТЕХЭКСПЕРТ». —Текст: электронный.
20. Фленов, М.Е. Linux глазами хакера. 5-е изд. / М.Е. Фленов. — СПб. : БХВ-Петербург, 2019. —416 с.
21. Лав, Р. Linux. Системное программирование. 2-е изд. / Р. Лав. — СПб. : Питер, 2014. — 448 с.
22. Уорд, Б. Внутреннее устройство Linux. / Б. Уорд. — СПб. : Питер, 2016. — 384 с.
23. Yosifovich, P. Windows Internals Seventh Edition. Part 1 / P. Yosifovich, A. Ionescu, M.E. Russinovich, D.A. Solomon. — Microsoft Press, 2017. — 784 p.
24. Intel 64 and IA-32 Architectures Software Developer’s Manual [Электронный ресурс] — Электрон. текстовые дан. —Последнее обновление : 16.11.2020. — Режим доступа: https://software.intel.com/content/www/us/en/develop/articles/intel-sdm.html.

9. Материально-техническая база, необходимая для осуществления образовательного процесса по дисциплине

Материально-техническая база, необходимая для осуществления образовательного процесса по дисциплине включает в свой состав специальные помещения:

-учебные аудитории для проведения занятий лекционного типа;

-учебные аудитории для проведения лабораторных работ, оснащенные средствами вычислительной техники, поддерживающими программное обеспечение, указанное в пункте 6;

- учебные аудитории для проведения групповых и индивидуальных консультаций;

- учебные аудитории для проведения текущего контроля и промежуточной аттестации;

- помещения для самостоятельной работы;

- помещения для хранения и профилактического обслуживания технических средств обучения.

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

Число посадочных мест в лекционной аудитории больше либо равно списочному составу потока, а в аудитории для практических занятий (семинаров) – списочному составу группы обучающихся.

Автор(ы):

Канд. физ.-мат. наук Мурин Д. М.

Приложение №1 к рабочей программе дисциплины
«Безопасность в современной информационной среде»

Фонд оценочных средств
для проведения текущей и промежуточной аттестации студентов
по дисциплине

1. Типовые контрольные задания или иные материалы, необходимые для оценки знаний, умений, навыков и (или) опыта деятельности, характеризующих этапы формирования компетенций

1.1 Контрольные задания и иные материалы, используемые в процессе текущей аттестации

Тест по теме 1.1 Правовые основы обеспечения информационной безопасности

1. Какие положения, связанные с вопросами обработки информации, закреплены в Конституции Российской Федерации?
   а) Право на неприкосновенность личной и семейной тайны.
   б) Право на обработку любой информации любым возможным способом.
   в) Запрет на обработку информации о частной жизни лица без его согласия.
   г) Право на получение гражданами допуска к государственной тайне.
2. Какие виды информации обязательно требуется защищать в соответствии с законодательством Российской Федерации:
   а) Информация для служебного пользования.
   б) Персональные данные.
   в) Государственная тайна.
   г) Врачебная тайна.
   д) Все перечисленные.
3. В соответствии с Федеральным законом «Об информации, информационных технологиях и защите информации» информация – это:
   а) Любые данные, представленные на материальном носителе.
   б) Сведения (сообщения, данные), независимо от формы их представления.
   в) Не энергия и не материя.
   г) Сведения, воспринимаемые человеком и (или) специальными устройствами как отражение фактов материального или духовного мира в процессе коммуникации.
4. Что из перечисленного можно рассматривать как базу данных в соответствии с законодательством Российской Федерации:
   а) EXCEL таблицу с упорядоченной и структурированной информацией.
   б) Файл формата DOC, в котором создан список слушателей этой программы.
   в) Картотеку регистратуры учреждения здравоохранения.
   г) Все перечисленные.
5. Целостность информации – это:
   а) Обязательное для выполнения лицом, получившим доступ к определенной информации, требование не передавать такую информацию третьим лицам без согласия ее обладателя.
   б) Состояние информации, при котором отсутствует любое ее изменение либо изменение осуществляется только преднамеренно субъектами, имеющими на него право.
   в) Возможность получения информации и ее использования.
6. На территории Российской Федерации запрещено распространение:

а) Информации, которая направлена на пропаганду войны.
б) Коммерческой тайны.
в) Информации, которая направлена на разжигание религиозной ненависти.
г) Персональных данных.

7. Гражданин или юридическое лицо, осуществляющие деятельность по эксплуатации информационной системы, в том числе по обработке информации, содержащейся в ее базах данных – это:
   а) Обладатель информации.
   б) Оператор информационной системы.
8. Если не определено иного, оператором информационной системы является:
   а) Обладатель информации.
   б) Собственник используемых для обработки содержащейся в базах данных информации технических средств.
   в) Лицо, определяющее цели обработки информации и осуществляющее обработку информации.
9. Не может быть ограничен доступ:
   а) К информации о состоянии окружающей среды.
   б) К персональным данным государственных гражданских служащих.
   в) К информации, хранящейся в открытых фондах библиотек.
   г) К сведениям о золотовалютных запасах Российской Федерации.
10. Какую ответственность может повлечь нарушение требований Федеральных законов:
   а) Уголовную.
   б) Дисциплинарную.
   в) Административную.
   г) Гражданско-правовую.
   д) Все перечисленные.

Тест по теме 1.2 Защита персональных данных

1. Персональные данные – это:
   а) Сведения о субъекте персональных данных не зависимо от формы их представления.
   б) Любая информация, относящаяся к прямо или косвенно определенному или определяемому физическому лицу (субъекту персональных данных).
   в) Любая информация, относящаяся к определенному или определяемому физическому лицу (субъекту персональных данных).
   г) Любая информация, относящаяся к определенному или определяемому на основании такой информации физическому лицу (субъекту персональных данных), в том числе его фамилия, имя, отчество, год, месяц, дата и место рождения, адрес, семейное, социальное, имущественное положение, образование, профессия, доходы, другая информация.
2. На какие отношения не распространяется действие федерального закона «О персональных данных»?
   а) На обработку персональных данных, отнесенных в установленном порядке к сведениям, составляющим государственную тайну.
   б) На обработку персональных данных, необходимую для осуществления прав и законных интересов оператора или третьих лиц.
   в) На обработку персональных данных, необходимую для исполнения судебного акта.

г) На обработку персональных данных физическими лицами исключительно для личных и семейных нужд, если при этом не нарушаются права субъектов персональных данных.

д) На обработку персональных данных, подлежащих опубликованию или обязательному раскрытию в соответствии с федеральным законом.

е) На обработку персональных данных, необходимую для организации хранения, комплектования, учета и использования содержащих персональных данных архивных документов в соответствии с законодательством об архивном деле в Российской Федерации.

3. Федеральный закон «О персональных данных» регулирует отношения, связанные:

а) Исключительно с обработкой персональных данных с использованием средств автоматизации.

б) С обработкой персональных данных, независимо от того обрабатываются ли они с использованием средств автоматизации или нет.

в) С обработкой персональных данных с использованием средств автоматизации, а также с обработкой персональных данных без использования средств автоматизации, если такая обработка соответствует характеру действий, совершаемых с персональными данными с использованием средств автоматизации.

г) С обработкой персональных данных без использования средств автоматизации.

4. Действия, в результате которых становится невозможным без использования дополнительной информации определить принадлежность персональных данных конкретному субъекту персональных данных, – это:

а) Блокирование персональных данных.

б) Уничтожение персональных данных.

в) Обезличивание персональных данных.

г) Перевод персональных данных на архивное хранение.

5. Действия, в результате которых *временно* прекращается обработка персональных данных, – это:

а) Блокирование персональных данных.

б) Уничтожение персональных данных.

в) Обезличивание персональных данных.

г) Перевод персональных данных на архивное хранение.

6. Какие из перечисленных действий с персональными данными являются обработкой персональных данных:

а) Хранение персональных данных.

б) Запись персональных данных.

в) Обезличивание персональных данных.

г) Удаление персональных данных.

7. С точки зрения федерального закона «О персональных данных» оператор – это:

а) Государственный орган, муниципальный орган, юридическое или физическое лицо, самостоятельно или совместно с другими лицами организующие и (или) осуществляющие обработку ПДн, а также определяющие цели обработки ПДн, состав ПДн, подлежащих обработке, действия (операции), совершаемые с ПДн.

б) Гражданин или юридическое лицо, осуществляющие деятельность по эксплуатации информационной системы, в том числе по обработке информации, содержащейся в ее базах данных.

8. Обработка персональных данных:

а) Не допускается без согласия субъекта персональных данных.

б) Должна ограничиваться достижением конкретных, заранее определенных и законных целей.

в) Не допускается в случаях несовместимых с целями сбора персональных данных.

г) Должна осуществляться на законной и справедливой основе.

9. Обработка персональных данных допускается:

а) С согласия субъекта персональных данных на обработку его персональных данных.

б) В случаях, если она необходима для исполнения судебного акта.

в) В случаях, если она необходима для осуществления профессиональной деятельности журналиста и (или) законной деятельности средства массовой информации.

г) В случаях, если ведется обработка персональных данных, подлежащих опубликованию в соответствии с законодательством Российской Федерации.

10. Кто несет ответственность за действия юридического лица, которому поручена обработка персональных данных, перед субъектом персональных данных?

а) Оператор.

б) Юридическое лицо, которому поручили обработку.

в) Никто.

г) Роскомнадзор.

11. В поручении обработки должны быть обязательно определены и указаны:

а) Цели обработки персональных данных.

б) Субъекты персональных данных, чьи персональные данные будут обрабатываться по поручению.

в) Требования к защите обрабатываемых персональных данных.

г) Средства защиты информации, которые необходимо применять юридическому лицу, которому поручена обработка персональных данных.

12. На ком лежит обязанность по доказательству получения согласия от субъекта персональных данных?

а) На Роскомнадзоре.

б) На юридическом лице, которому поручили обработку.

в) Ни на ком.

г) На операторе.

13. Согласие субъекта персональных данных должно включать:

а) Паспортные данные субъекта персональных данных или его законного представителя.

б) Контактные данные лица, ответственного за организацию обработки персональных данных.

в) Адрес оператора.

г) Фамилии, имена и отчества физических лиц, которые осуществляют обработку персональных данных по поручению оператора.

14. В случае смерти субъекта персональных данных:

а) Получать согласие на обработку его персональных данных требуется у наследников субъекта персональных данных.

б) Получать согласие на обработку его персональных данных требуется у Роскомнадзора.

в) Получать согласие на обработку его персональных данных не требуется.

15. К специальным категориям персональных данных относятся:

а) Сведения, касающиеся расовой принадлежности.

б) Сведения, касающиеся гражданства.

в) Сведения, касающиеся политических взглядов.

г) Сведения, касающиеся инвалидности.

16. С точки зрения федерального закона «О персональных данных» к биометрическим персональным данным относятся:

а) Все сведения, которые характеризуют физиологические и биологические особенности человека, на основании которых можно установить его личность.

б) Сведения, которые вносятся в базу биометрических данных граждан Российской Федерации.

в) Все сведения, которые характеризуют физиологические и биологические особенности человека, на основании которых можно установить его личность, и которые используются для установления его личности.

17. Кто обязан убедиться в том, что иностранным государством, на территорию которого осуществляется передача персональных данных, обеспечивается адекватная защита прав субъектов персональных данных?

    а) Оператор.

    б) Юридическое лицо, которому поручили обработку.

    в) Никто.

    г) Роскомнадзор.

18. Субъект персональных данных имеет право на получение следующей информации, касающейся обработки его персональных данных:

    а) Правовые основания и цели обработки персональных данных.

    б) Поименный перечень сотрудников оператора, которые имеют доступ к его персональным данным.

    в) Сведения об осуществленной или о предполагаемой трансграничной передаче данных.

    г) Сведения о применяемых оператором средствах защиты информации.

19. Право гражданина на получение информации, касающейся обработки его персональных данных, может быть ограничено:

    а) На основании заявления другого субъекта персональных данных.

    б) В случаях, если обработка персональных данных осуществляется в случаях, предусмотренных законодательством Российской Федерации о транспортной безопасности.

    в) В случаях, если обработка персональных данных осуществляется в целях обороны страны, безопасности государства и охраны правопорядка.

    г) В случаях, если обработка персональных данных осуществляется в рамках законной деятельности средства массовой информации.

20. Контроль и надзор за выполнением мер по обеспечению безопасности персональных данных осуществляет (осуществляют):

    а) Минкомсвязи России.

    б) Роскомнадзор.

    в) ФСБ России.

    г) ФСТЭК России.

21. Какой орган государственной власти имеет право ознакомления с персональными данными при осуществлении контрольных и проверочных мероприятий?

    а) ФСБ России.

    б) Роскомнадзор.

    в) ФСТЭК России.

22. Лица, виновные в нарушении положений законодательства Российской Федерации в области персональных данных при обработке персональных данных работника, могут быть привлечены:

    а) К уголовной ответственности.

    б) К дисциплинарной ответственности.

    в) К административной ответственности.

    г) К материальной ответственности.

Тест по теме 1.3 Организационные основы обеспечения информационной безопасности

1. Расположите в правильном порядке этапы работ по обеспечению безопасности информации.
   1) Оценка соответствия объекта информатизации.
   2) Выявление и анализ информационных активов.
   3) Проектирование (разработка) системы защиты информации.
   4) Формирование требований к защите информации.
   5) Внедрение системы защиты информации.
   6) Эксплуатация системы защиты информации.

   а) 1) 2) 3) 4) 5) 6).
   б) 4) 2) 3) 5) 1) 6).
   в) 2) 4) 3) 5) 6) 1).
   г) 2) 4) 3) 5) 1) 6).
2. Пусть не обезличенные персональные данные о состоянии здоровья всех граждан Ярославской области обрабатываются в информационной системе, для которой актуальны угрозы связанные с эксплуатацией уязвимостей в прикладном, но не в системном программном обеспечении. Какой уровень защищенности должен быть установлен для таких персональных данных?
   а) УЗ1.
   б) УЗ2.
   в) УЗ3.
   г) УЗ4.
3. Пусть не обезличенные персональные данные в том числе фотография сотрудников небольшого (до 10 000 сотрудников) предприятия обрабатываются в системе контроля и управления доступом, для которой актуальны угрозы не связанные с эксплуатацией уязвимостей в прикладном и системном программном обеспечении. Какой уровень защищенности должен быть установлен для таких персональных данных?
   а) УЗ1.
   б) УЗ2.
   в) УЗ3.
   г) УЗ4.
4. Внешние нарушители реализуют угрозы:
   а) Из внешних сетей связи общего пользования.
   б) Непосредственно в информационных системах.
   в) Из сетей международного информационного обмена.
   г) Находясь в пределах контролируемой зоны.
5. Примерами внешних нарушителей могут являться:
   а) Пользователи информационной системы.
   б) Конкурирующие организации.
   в) Недобросовестные партнеры.
   г) Обслуживающий персонал организации.
6. Примерами внутренних нарушителей могут являться:
   а) Администраторы безопасности информационных систем.
   б) Сторонние физические лица.
   в) Лица, обеспечивающие сопровождение программного обеспечения.
   г) Криминальные структуры.
7. К объективным угрозам относятся:
   а) Ошибки обслуживающего персонала.

б) Дефекты, сбои и отказы, аварии технических средств и систем объектов информатизации, а так же систем обеспечения объектов информатизации.

в) Природные явления, стихийные бедствия.

г) Факторы социально-политического характера.

8. Угрозы утечки информации возможны посредством:

а) Воздействия программными средствами в комплексе с преднамеренным силовым электромагнитным воздействием.

б) Передачи информации по открытым каналам связи.

в) Подключения к техническим средствам и системам объекта информатизации.

г) Обработки информации на незащищенных технических средствах обработки информации.

9. Угрозы несанкционированного доступа к информации, реализуются путем:

а) Копирования информации на незарегистрированный носитель информации.

б) Хищения носителя защищаемой информации.

в) Использования программного обеспечения технических средств информационной системы, через применение вредоносного программного кода.

г) Силового электромагнитного воздействия по проводным линиям связи на порты ввода-вывода сигналов и порты связи.

10. Какие средства защиты информации обычно применяются для обеспечения безопасности информации, обрабатываемой на автономных компьютерах:

а) Средства защиты информации от несанкционированного доступа.

б) Межсетевые экраны.

в) Средства криптографической защиты информации.

г) Средства антивирусной защиты.

д) Системы обнаружения вторжений.

11. Какие средства защиты информации позволяют обеспечить безопасность информации, передаваемой по каналам связи, выходящим за пределы контролируемой зоны:

а) Средства защиты информации от несанкционированного доступа.

б) Межсетевые экраны.

в) Средства криптографической защиты информации.

г) Системы обнаружения вторжений.

12. Какой вид средств защиты информации позволяет контролировать различные каналы передачи информации: электронную почту, месенджеры, съемные носители информации?

а) IPS.

б) DLP.

в) IDS.

г) CSP.

13. Аттестация объектов информатизации – это:

а) Документальное удостоверение соответствия продукции или иных объектов, процессов проектирования, производства, строительства, монтажа, наладки, эксплуатации, хранения, перевозки, реализации и утилизации, выполнения работ или оказания услуг требованиям технических регламентов, положениям стандартов, сводов правил или условиям договоров.

б) Прямое или косвенное определение соблюдения требований, предъявляемых к объекту защиты.

в) Официальное признание компетентности физического или юридического лица выполнять работы в определенной области.

г) Комплекс организационно-технических мероприятий, в результате которых посредством специального документа подтверждается, что объект соответствует

требованиям стандартов или иных нормативно-технических документов по безопасности информации.

14. Какой документ дает право обработки информации с указанным в нем уровнем конфиденциальности?
    1) Лицензия.
    2) Аттестат аккредитации.
    3) Сертификат.
    4) Аттестат соответствия.
15. На настоящий момент срок действия аттестата соответствия информационной системы, в которой обрабатывается конфиденциальная информация, в случае, если в ходе ее эксплуатации, в нее не вносятся существенные изменения, составляет:
    а) 3 года.
    б) 5 лет.
    в) Весь срок эксплуатации информационной системы.
16. Тестирование на проникновение – это скорее:
    а) Анализ уязвимостей информационной системы.
    б) Испытания системы защиты информации путем осуществления попыток несанкционированного доступа (воздействия) к информационной системе.

Тест по теме 2.1 Архитектура компьютера

1. За непосредственное выполнение операции в процессоре отвечает:
    а) Арифметико-логическое устройство.
    б) Кэш-память.
    в) Блок управления.
    г) Регистры.
2. Используя 10 бит для адресации ячеек памяти размером 1 байт, мы сможем обеспечить адресацию следующего объема памяти:
    а) 10 байт.
    б) 80 байт.
    в) 1024 байт.
    г) 1024 бит.
3. Расположите в порядке увеличения объема памяти.
    а) Страница.
    б) Бит.
    в) Слово.
    г) Банк.
    д) Ячейка.
4. Расположите виды памяти в порядке увеличении скорости работы.
    а) Регистры процессора.
    б) Твердотельные накопители.
    в) Основная (оперативная) память.
    г) Оптические диски.
    д) Магнитные жесткие диски.
    е) Кэш-память.
5. Какая концепция обычно реализуется в процессорах видеокарт?
    а) Множественный поток команд, множественный поток данных.
    б) Одиночный поток команд, множественный поток данных.
    в) Множественный поток команд, одиночный поток данных.
    г) Одиночный поток команд, одиночный поток данных.
6. Для современных магнитных жестких дисков характерно:
    а) Большая стоимость по отношению к твердотельным накопителям.

б) Постепенное изнашивание транзисторов.
в) Наличие механических элементов.
г) Расположение контроллера на материнской плате.
д) Больший объем памяти по сравнению с твердотельными накопителями.

7. Какая шина наиболее распространена на текущий момент в персональных компьютерах:
   а) ISA.
   б) PCI.
   в) PCI Express.
   г) SCSI.
8. Пусть тактовая частота шины компьютера составляет 5 ГГц. За один такт по шине можно передать 16 бит. Оцените скорость передачи информации по шине?
   а) 80 Мегабит в секунду.
   б) 10 Гигабайт в секунду.
   в) 80 Гигабайт в секунду.
   г) 21 Гигабайт в секунду.
9. Для проекционно-емкостных сенсорных экранов характерно:
   а) Высокая скорость отклика при касании.
   б) Возможность управления различными устройствами.
   в) Поддержка multi-touch.
   г) Невозможность определения силы нажатия.
   д) Проблема «двоения».
10. Элементами жидкокристаллического монитора являются:
    а) Лучевая трубка.
    б) Источник света.
    в) ЖК-матрица.
    г) ПЗС-матрица.
    д) Электроды.
11. Какой элемент принтера отвечает за фиксацию тонера на бумаге:
    а) Фотовал.
    б) Термовал.
    в) Ролик переноса.
    г) Вал подачи тонера.
12. Назначением лазера в цветном принтере является:
    а) Нанесение тонера на фотовал.
    б) Фиксация тонера на бумаге.
    в) Удаление несущих заряд элементов с фотовала.
    г) Подача бумаги в принтер.
13. Элементами цифровой веб-камеры являются:
    а) Фотопленка.
    б) Объектив.
    в) ПЗС-матрица.
    г) Фикс-фокус
    д) Процессор.
14. Для конденсаторных микрофонов характерно:
    а) Слабая чувствительность.
    б) Устойчивость к ударам.
    в) Высокая чувствительность.
    г) Зависимость от параметров окружающей среды (температуры, влажности).
    д) Применение в студиях звукозаписи.

Тест по теме 3.1 Введение в информационную безопасность операционных систем

1. Пусть в ОС реализовано дискреционное управление доступом со следующими правами: чтение(r), запись(w) и исполнение(x). Присутствует файл приложения «Калькулятор.exe» со следующим списком доступа: (Алиса: rwx), (Борис: rx). Выберите правильные утверждения:
   а) Алиса может запустить приложение «Калькулятор.exe».
   б) Борис не может запустить приложение «Калькулятор.exe».
   в) Алиса не может изменить содержимое файла «Калькулятор.exe».
   г) Борис может изменить содержимое файла «Калькулятор.exe».
2. Пусть в ОС реализовано групповое управление доступом со следующими правами: чтение(r), запись(w) и исполнение(x). Присутствует файл «Накладная.docx» со следующим списком доступа: (Бухгалтеры: rw), (Курьеры: r), (Алиса: rw). В системе заданы роли, в которые включены соответствующие пользователи: (Бухгалтеры: Борис, Галина), (Курьеры: Виктор). Выберите правильные утверждения:
   а) Борис не может изменить содержимое файла «Накладная.docx».
   б) Галина может читать содержимое файла «Накладная.docx».
   в) Виктор может изменить содержимое файла «Накладная.docx».
   г) Виктор может читать содержимое файла «Накладная.docx».
   д) Алиса может изменить содержимое файла «Накладная.docx».
3. Пусть в ОС реализовано мандатное управление доступом. Присутствует файл «log.txt» с уровнем секретности 1. Присутствуют пользователи Алиса с уровнем допуска 1, Борис с уровнем допуска 2 и Виктор с уровнем допуска 0. Выберите правильные утверждения:
   а) Виктор может изменить содержимое файла «log.txt».
   б) Виктор может читать содержимое файла «log.txt».
   в) Алиса может изменить содержимое файла «log.txt».
   г) Алиса может читать содержимое файла «log.txt».
   д) Борис может изменить содержимое файла «log.txt».
   е) Борис может читать содержимое файла «log.txt».
4. Пусть в ОС реализована модель целостности Биба. Присутствует файл «log.txt» с уровнем целостности 1. Присутствуют пользователи Алиса с уровнем целостности 1, Борис с уровнем целостности 2 и Виктор с уровнем целостности 0. Выберите правильные утверждения:
   а) Виктор может изменить содержимое файла «log.txt».
   б) Алиса может изменить содержимое файла «log.txt».
   в) Борис может изменить содержимое файла «log.txt».
   г) Все трое могут читать содержимое файла «log.txt».
5. Выберите правильные утверждения о аутентификации в современных ОС:
   а) Пароли пользователя хранятся на диске, на котором установлена система, в первоначальном виде.
   б) Эталонные значения, необходимые для прохождения биометрической аутентификации, хранятся в системе в недостаточном для восстановления изначальных биометрических данных объеме.
   в) Токен физически изготовлен таким образом, что считывание с него закрытого ключа является невозможной или дорогостоящей операцией.
   г) Для аутентификации с помощью токена в системе должен присутствовать открытый ключ пользователя, соответствующий закрытому ключу на его токене.
6. Что не входит в метаданные файла (выберите один вариант)?
   а) Время создания файла.
   б) Адрес корневой директории.
   в) Время модификации файла.

г) Адреса кластеров содержимого файлов.

д) Информация о владельце файла.

7. Выберите верные утверждения о управлении памятью в современных ОС:

а) Современные ОС используют виртуальную память.

б) Современные ОС не защищают память одних процессов от чтения другими процессами.

в) Современные ОС разделяют общую память между процессами, часто в такой памяти находятся библиотеки.

г) Современные ОС никогда не выгружают части оперативной памяти на диск во время работы.

д) В современных ОС память разбита на маленькие фрагменты, называемые страницами.

8. Выберите верные утверждения о планировщике:

а) Планировщик выделяет процессорное время короткими интервалами, называемыми квантами.

б) В случае исполнения процессом инструкции, для завершения которой требуется длительное ожидание, планировщик переводит процесс в состояние «заблокирован» и не будет выделять ему процессорное время, пока состояние не сменится на «готов».

в) Для работы планировщика процессы должны сами передавать на него управление, так как компьютеры не предоставляют ОС механизма для периодического прерывания выполнения пользовательского процесса.

г) В планировании по приоритетам все процессы с разными приоритетами получают примерно одинаковое количество времени.

9. Выберите верное утверждение (выберите один вариант):

а) ОС реализована аппаратно в процессоре.

б) ОС реализована аппаратно в материнской плате.

в) ОС – программное обеспечение, которое предоставляет приложениям ресурсы аппаратного обеспечения компьютера в виде удобных абстракций, но не управляет этим аппаратным обеспечением.

г) ОС – программное обеспечение, которое предоставляет приложениям ресурсы аппаратного обеспечения компьютера в виде удобных абстракций и управляет этим аппаратным обеспечением.

10. Выберите верное утверждение (выберите один вариант):

а) В ОС компьютера с одноядерным процессором в каждый момент времени может работать только один процесс.

б) В ОС компьютера с одноядерным процессором у процессов всегда присутствует только один поток.

в) В ОС компьютера с многоядерным процессором в конкретный момент времени могут выполнятся несколько потоков одного процесса.

г) В ОС компьютера с многоядерным процессором конкретный процесс может использовать только одно ядро процессора.

Тест по теме 3.2 Информационная безопасность операционных систем семейства Windows

1. На основе каких данных субъекта ОС Windows принимает решение о доступе?

а) Хеш значение пароля пользователя, запустившего процесс.

б) Токен перевоплощения.

в) Идентификатор процесса.

г) Токен доступа.

д) Базовый приоритет процесса.

2. На основе каких данных объекта ОС Windows принимает решение о доступе?
   а) Привилегии.
   б) Токен доступа.
   в) Дескриптор безопасности.
   г) Системный список управления доступом.
   д) Способ аутентификации пользователя.
3. Какие примитивные права объединяет в себе право чтения ОС Windows?
   а) «Чтение атрибутов безопасности».
   б) «Чтение системных атрибутов», «чтение атрибутов безопасности».
   в) «Чтение данных».
   г) «Чтение системных атрибутов», «чтение атрибутов безопасности», «чтение данных».
   д) «Чтение системных атрибутов», «чтение атрибутов безопасности», «чтение данных», «выполнение файлов» и «переход в директорию».
4. Выберите правильные утверждения о мандатной политике «Не-Записывать-Вверх» ОС Windows:
   а) Обеспечивает свойство целостности данных.
   б) Обеспечивает свойство конфиденциальности данных.
   в) Используется в системе только для объектов сетевых сокетов.
   г) Неявно используется для всех NTFS-файлов.
   д) Разрешает доступ на запись только субъектам с уровнем целостности равным или большим по отношению к уровню целостности объекта доступа.
5. Какие из перечисленных прав ОС Windows предоставляет по умолчанию владельцу файла?
   а) Читать ССУД.
   б) Читать ДСУД.
   в) Читать содержимое файла.
   г) Изменять ДСУД.
   д) Изменять ССУД.
   е) Изменять содержимое файла.
6. Выберете правильные утверждения относительно алгоритма определения правомерности доступа ОС Windows:
   а) Первым действием является проверка соответствия доступа мандатной политике.
   б) Проверка соответствия доступа мандатной политике осуществляется после анализа записей ДСУД.
   в) Если при последовательном анализе записей ДСУД оказывается, что одно из запрашиваемых прав запрещается в текущей записи, то доступ запрещается.
   г) Если при последовательном анализе записей ДСУД разрешающие права текущей записи в сумме с разрешающими правами предыдущих записей перекрыли все запрашиваемые права, то доступ разрешается.
   д) Если в списках ДСУД не было запрещающих запрашиваемые права записей, и в то же время все разрешающие записи не перекрыли запрашиваемые права, то доступ запрещается.
7. Какая привилегия ОС Windows позволяет читать любой файл вне зависимости от заданных прав?
   а) Привилегия создания резервных копий.
   б) Привилегия изменения системного времени.
   в) Привилегия завершения работы системы.
   г) Привилегия увеличения рабочего набора.
   д) Привилегия создания файла подкачки.
8. Выберите сущности, не входящие в токен доступа в ОС Windows:

а) SID пользователя.
б) ДСУД всех объектов системы.
в) SID-ы групп.
г) ССУД всех объектов системы.
д) Привилегии.

9. Выберите сущности, входящие в дескриптор безопасности объекта в ОС Windows:
   а) SID владельца объекта.
   б) Дискреционный список управления доступом.
   в) Системный список управления доступом.
   г) Список токенов доступа процессов, осуществляющих доступ к объекту.
   д) Уровень целостности.
10. Какие из пунктов правильно описывают фильтрованный токен доступа администратора в ОС Windows?
   а) Уровень целостности устанавливается средним.
   б) Уровень целостности устанавливается высоким.
   в) Список привилегий, которые могут попасть в фильтрованный токен, сильно ограничен.
   г) При определении правомерности доступа среди записей ДСУД с SID административных групп будут учтены только запрещающие.
   д) Списки привилегий одинаковы в обычном и фильтрованном токене доступа администратора.

Тест по теме 3.2 Информационная безопасность операционных систем семейства Linux

1. На основе каких данных субъекта ОС Linux принимает решение о доступе?
   а) SUID-бит.
   б) Sticky-бит.
   в) Учетные данные.
   г) UID процесса.
   д) Электронная подпись программы.
2. Какие права присутствуют в ОС Linux:
   а) Исполнение.
   б) Чтение i-node.
   в) Чтение.
   г) Удаление.
   д) Запись.
3. Для чего служит SUID-бит в ОС Linux?
   а) Позволяет запустить приложение от имени владельца файла приложения.
   б) Позволяет запустить приложение от имени суперпользователя.
   в) Позволяет запустить приложение с привилегией CAP_SYS_ADMIN.
   г) Позволяет запустить приложение с UID равным нулю.
   д) Запрещает запуск приложения всем пользователям, кроме суперпользователя.
4. Что делает маска в списке управления доступом файла в ОС Linux?
   а) Задает максимальные права, которые можно получить из записей для групп.
   б) Задает максимальные права, которые можно получить из записи остальных.
   в) Задает максимальные права, которые можно получить из записи владельца файла.
   г) Задает максимальные права, которые можно получить из записей для пользователей и групп.

д) Задает максимальные права, которые можно получить из записей для пользователей.

5. Что такое соль хеш-значения пароля в ОС Linux?

а) Строка, которая выбирается при каждой аутентификации случайно для обеспечения безопасности пароля.

б) Случайно выбранная при создании пароля строка, которая склеивается с хеш-значением после вычисления хеш-функции.

в) Случайно выбранная при создании пароля строка, которая склеивается с паролем перед вычислением хеш-функции.

г) Длина, до которой урезается пароль пользователя для компактного хранения в системе.

6. Выберите сущности, входящие в учетные данные процесса в ОС Linux:

а) UID пользователя, запустившего процесс.

б) Группы пользователя, запустившего процесс.

в) Привилегии.

г) Права исполняемого файла, из которого был запущен процесс.

д) Флаг эффективности привилегий.

7. Выберите сущности, входящие в атрибуты безопасности файла в ОС Linux:

а) Тройка прав для каждой группы в системе.

б) Привилегии.

в) Тройка прав владельца файла.

г) Тройка прав пользователей, не являющихся владельцами файла и не входящих в группу владельца файла по умолчанию.

д) Владелец файла.

8. Выберите сущности, входящие в атрибуты безопасности файла в ОС Linux:

а) Тройка прав для каждой группы в системе.

б) Привилегии.

в) Тройка прав владельца файла.

г) Тройка прав пользователей, не являющихся владельцами файла и не входящих в группу владельца файла по умолчанию.

д) Владелец файла.

9. Какие наборы привилегий есть у файла в ОС Linux:

а) Наследуемые.

б) Эффективные.

в) Внешние.

г) Ограничивающие.

д) Разрешенные.

10. Какую хеш-функцию использует ОС Linux для вычисления хеш-значения пароля в ОС Linux?

а) MD-5.

б) SHA-256.

в) SHA-512.

г) SHA-3.

д) Функций несколько, около хеш-значения пароля хранится номер использованной хеш-функции.

11. Что делает конвейер в ОС Linux?

а) Фильтрует вывод команды.

б) Перенаправляет стандартный вывод команды с консоли стандартный на вход другой команде.

в) Поднимает права до прав суперпользователя.

г) Откладывает выполнение команды на указанный срок.

Тест по теме 4.1 Введение в архитектуру локальных вычислительных сетей

1. Какой порядок уровней модели OSI верный?
   а) Физический, канальный, транспортный, сетевой, сеансовый, представления, прикладной.
   б) Физический, канальный, сетевой, транспортный, сеансовый, представления, прикладной.
   в) Физический, канальный, сетевой, транспортный, сеансовый, прикладной, представления.
   г) Физический, канальный, транспортный, сетевой, сеансовый, прикладной, представления.
2. Какие протоколы относятся к транспортному уровню модели OSI?
   а) UDP.
   б) ARP.
   в) IPv4.
   г) GSM.
   д) TCP.
   е) DNS.
   ж) PPTP.
3. Какой уровень предназначен для определения пути передачи данных?
   а) Физический.
   б) Сеансовый.
   в) Транспортный.
   г) Представления.
   д) Канальный.
   е) Прикладной.
   ж) Сетевой.
4. Какие флаги используются в протоколе TCP для установления соединения?
   а) RST.
   б) SYN.
   в) FIN.
   г) URG.
   д) ACK.
   е) PSH.
5. Какие преимущества есть у FTTB?
   а) Высокая скорость работы Интернет.
   б) Равная скорость приема и передачи информации.
   в) Независимость скорости доступа от числа абонентов, подключенных к коммутатору.
   г) Отсутствие необходимости размещения коммутатора провайдера в здании.
6. Какие недостатки есть у FTTB?
   а) Низкая скорость работы Интернет.
   б) Разная скорость приема и передачи информации.
   в) Зависимость скорости доступа от числа абонентов, подключенных к коммутатору.
   г) Необходимость размещения коммутатора провайдера в здании.
7. Выберите верные утверждения
   а) TCP не гарантирует доставку датаграмм.
   б) UDP не гарантирует доставку датаграмм.
   в) UDP гарантирует доставку датаграмм.
   г) TCP гарантирует доставку датаграмм.
8. Какой адрес относится к адресному пространству IPv4?

а) 192.168.0.17
б) 129.256.0.0
в) 301.169.107.0.0.3
г) 127.0.1000.0

9. Как работает концентратор (хаб)?
   а) При получении пакета данных хаб пересылает этот пакет на все остальные свои порты.
   б) При получении пакета данных хаб пересылает этот пакет на порт в соответствии с таблицей MAC-адресов. Если соответствия нет, пакет отбрасывается.
   в) При получении пакета данных хаб пересылает этот пакет на порт в соответствии с таблицей MAC-адресов. Если соответствия нет, в сеть отправляется ARP-запрос.
10. Как работает коммутатор?
   а) В случае, если для отправляемого MAC-адреса нет соответствия, коммутатор рассылает пакеты на все порты, кроме порта-получателя.
   б) При получении пакета данных коммутатор пересылает этот пакет на все остальные свои порты.
   в) Коммутатор хранит в памяти таблицу коммутации, в которой указано сопоставление MAC-адреса и номера порта коммутатора.
   г) Со временем коммутатор строит таблицу для всех активных MAC-адресов.
   д) Таблица MAC-адресов коммутатора статична и настраивается вручную.

Тест по теме 4.2 Сетевые угрозы и методы противодействия им

1. Какие бывают источники возникновения уязвимостей?
   а) Ошибки реализации.
   б) Ошибки обслуживания.
   в) Ошибки проектирования.
   г) Ошибки HR-отдела.
2. Что не входит в базовую группу метрик CVSS?
   а) Способ получения доступа.
   б) Влияние на конфиденциальность.
   в) Влияние на пользователя.
   г) Показатель аутентификации.
   д) Сложность получения доступа.
3. Какой группы метрик CVSS не существует?
   а) Комплексная.
   б) Временная.
   в) Базовая.
   г) Контекстная.
4. Кем разработана CVSS?
   а) ISO.
   б) FIRST.
   в) WWW.
   г) UCLA.
5. Что не является метрикой в CVSS?
   а) Сложность атаки.
   б) Влияние на доступность.
   в) Длительность атаки.
   г) Способ получения доступа.
   д) Показатель аутентификации.

6. Что является пассивной атакой?
   а) Прослушивание трафика.
   б) Отказ в обслуживании.
   в) Физическое нападение на объект.
   г) Эксплуатация уязвимости.
7. Что такое эвристический анализ?
   а) Метод, предназначенный для обнаружения новых, еще не выявленных вирусов.
   б) Механизм, необходимый для отслеживания неизменности файлов, документов, реестра, конфигурации оборудования.
   в) Метод, основанный на последовательном просмотре памяти устройства, загрузочных секторов, файлов в поиске сигнатур известных вирусов.
8. Что такое бэкдор?
   а) Часть вредоносного программного обеспечения, реализованного для сокрытия присутствия этого вредоносного кода и его действий.
   б) Приложение, используемое для дальнейшей загрузки и запуска полноценного вредоносного программного обеспечения.
   в) Вредоносное программное обеспечение, которое, помимо получения контроля над зараженным устройством, пытается захватить под свой контроль другие узлы сети.
   г) Приложение, позволяющее управлять компьютером удаленно.
9. Что такое руткит?
   а) Часть вредоносного программного обеспечения, реализованного для сокрытия присутствия этого вредоносного кода и его действий.
   б) Приложение, используемое для дальнейшей загрузки и запуска полноценного вредоносного программного обеспечения.
   в) Вредоносное программное обеспечение, которое, помимо получения контроля над зараженным устройством, пытается захватить под свой контроль другие узлы сети.
   г) Приложение, позволяющее управлять компьютером удаленно.
10. Что следует делать, чтобы защитить себя от вирусов?
   а) Не запускать приложения из недоверенных источников.
   б) Следить за цифровыми подписями устанавливаемого программного обеспечения.
   в) Отключить межсетевой экран.
   г) Всегда открывать вложения электронной почты с темой «Важно» и «Срочно».
   д) Своевременно обновлять операционную систему и программное обеспечение.
   е) Использовать антивирусное программное обеспечение.

Тест по теме 4.3 Межсетевые экраны

1. Что такое межсетевой экран?
   а) Программное или программно-техническое средство, реализующее функции контроля и фильтрации в соответствии с заданными правилами проходящих через него информационных потоков.
   б) Устройство, предназначенное для соединения нескольких узлов компьютерной сети в пределах одного или нескольких сегментов сети.
   в) Устройство, которое позволяет организовать локальную сеть с возможностью выхода в интернет для других устройств.
2. Межсетевые экраны для веб-приложений располагают:

а) Перед защищаемым веб-сервером (трафик вначале передается межсетевому экрану, затем веб-серверу).

б) После защищаемого веб-сервера (трафик вначале передается веб-серверу, затем межсетевому экрану).

в) Межсетевой экран и защищаемый им веб-сервер находятся в разных подсетях, трафик между ними запрещен.

г) Вместо защищаемого веб-сервера.

3. Персональные межсетевые экраны для настольных компьютеров и ноутбуков:

а) Обеспечивают дополнительный уровень защиты от сетевых атак.

б) Полностью заменяют все остальные инструментальные средства обеспечения безопасности.

в) Полностью заменяют маршрутизаторы, являясь шлюзом по умолчанию для защищаемого компьютера или ноутбука.

г) Предоставляют все необходимые сетевые сервисы для защищаемого компьютера или ноутбука.

4. Персональные межсетевые экраны для настольных компьютеров и ноутбуков являются:

а) Аппаратно-программными средствами защиты.

б) Всегда встроенными в ОС, которую они защищают; не могут быть реализованы внешними производителями.

в) Исключительно программными.

г) Исключительно внешними, не встроенными в ОС, которую они защищают; всегда реализованы внешними производителями.

5. Персональные межсетевые экраны для настольных компьютеров и ноутбуков устанавливаются:

а) На хостах, которые они защищают.

б) На маршрутизаторах, которые указаны на хосте в качестве шлюза по умолчанию.

в) На отдельных компьютерах.

г) На конечных точках VPN.

6. Выберите несуществующий вид трансляции сетевых адресов.

а) Динамическая.

б) Статическая.

в) С использованием портов.

г) С использованием мостов.

7. Шлюзы уровня приложений позволяют:

а) Исключить прямое взаимодействие двух узлов путем реализации роли посредника.

б) Выполнять функции шлюза сеансового уровня.

в) Анализировать все существующие в мире протоколы.

г) Анализировать только поддерживаемые этим межсетевым экраном протоколы.

8. Управляемые коммутаторы могут:

а) Осуществлять фильтрацию на основе IP-адресов.

б) Осуществлять фильтрацию по используемому протоколу.

в) Осуществлять фильтрацию на основе MAC-адреса.

г) Осуществлять фильтрацию на основе VLAN ID.

9. Выберите возможности межсетевого экрана.

а) Регистрация событий и генерация отчетов.

б) Фильтрация трафика.

в) Трансляция сетевых адресов.

г) Аутентификация пользователей.

д) Администрирование.

10. Какие утверждения о программном межсетевом экране верны?

а) Подходит в случаях, когда устройство пользователя помещается в недоверенную среду.

б) При его работе используются ресурсы устройства, на котором он функционирует.

в) Подходит для задач сегментирования сетей.

г) Подходит для отделения доверенной части сети от внешних угроз.

д) Считается более отказоустойчивым, чем аппаратный межсетевой экран.

Тест по теме 5.1 Введение в криптографические методы защиты информации

1. Каждый шифротекст может быть получен как результат следующего преобразования:

а) E_k ($D_k(p)$).

б) $D_k(p)$.

в) $E_k(p)$.

г. D_k ($E_k(p)$).

2. Зашифруйте с помощью шифра «Атбаш» слово «World».

A	B	C	D	E	F	G	H	I	J	K	L	M
Z	Y	X	W	V	U	T	S	R	Q	P	O	N

а) Dlrow.

б) Svood.

в) Woild.

г) Dliow.

3. Рассшифруйте слово «Xjxob», зашифрованное с помощью шифра Гая Юлия Цезаря:

A	B	C	D	E	F	G	H	I	J	K	L	M	N	O	P	Q	R	S	T	U	V	X	Y	Z
X	Y	Z	A	B	C	D	E	F	G	H	I	J	K	L	M	N	O	P	Q	R	S	T	U	V

а) Tgtly.

б) Amare.

в) Crypt.

г) Vivna.

4. Зашифруйте слово «Жизнь» с помощью перестановки

1	2	3	4	5
2	5	3	1	4

а) Нжзьи.

б) Ьнзиж.

в) Нзьжи.

г) Иьзжн.

5. Расшифруйте слово «1216312611» с помощью таблицы Полибия:

	1	2	3	4	5	6
1	А	Б	В	Г	Д	Е
2	Ё	Ж	З	И	Й	К
3	Л	М	Н	О	П	Р
4	Ы	Е	У	Ф	Х	Ц
5	Ч	Ш	Щ	Ъ	Ы	Ь
6	Э	Ю	Я	*	*	*

а) Белка.

б) Ёэвюа.

в) Стрелка.
г) Белок.

6. Впервые метод частотного криптоанализа впервые изложил:
   а) Леон Баттиста Альберти.
   б) Франческо Симонетта.
   в) Абу Юсуф Якуб аль-Кинди.
   г) Джироламо Кардано.
7. Диск Альберти позволяет автоматизировать:
   а) Шифр простой замены (одноалфавитный шифр).
   б) Многоалфавитный шифр.
   в) Шифр перестановки.
   г) Поточный шифр.
8. Использование пароля для мнемонического запоминания перестановки символов алфавита предложил:
   а) Матео Ардженти.
   б) Блез де Виженер.
   в) Джованни Баттиста Беллазо.
   г) Джамбаттиста (Джованни) делла Порта.
9. Помещение для перлюстрации переписки в XVII – XX веках называлось:
   а) Белый кабинет.
   б) Тайная комната.
   в) Янтарная комната.
   г) Черный кабинет.
   д) Красный кабинет.
10. Шифры, в которых каждый символ открытого текста преобразуется в символ шифротекста, в зависимости от своего расположения в открытом тексте и ключа называются:
   а) Многоалфавитными шифрами.
   б) Блочными шифрами.
   в) Поточными шифрами.
   г) Роторными шифрами.
11. Зашифруйте слово «СЛОН» биграммным шифром Плейфера.

У	Ч	О	Ь	В
Ж	Т	Э	Н	Ф
Ш	Г	Л	Б	П
М	Я	Ц	З	Р
С	Е	А	Ы	К
Ю	Д	Щ	И	Х

   а) ВАЬИ.
   б) ШАЭЬ.
   в) ЭЩУЫ.
   г) ЫЦЦЗ.
12. Пусть перестановка T представлена следующей таблицей:

1	2	3	…	$n-5$	$n-4$	$n-3$	$n-2$	$n-1$	n
5	6	7	…	$n-1$	n	1	2	3	4

13. Какой вид имеет перестановка обратная перестановке T?
   а.

1	2	3	…	$n-5$	$n-4$	$n-3$	$n-2$	$n-1$	n
1	2	3	…	$n-5$	$n-4$	$n-3$	$n-2$	$n-1$	n

   б.

1	2	3	…	$n-5$	$n-4$	$n-3$	$n-2$	$n-1$	n
4	3	2	…	10	9	8	7	6	5

в.

1	2	3	…	$n-4$	$n-3$	$n-2$	$n-1$	n
4	5	6	…	$n-1$	n	1	2	3

г.

1	2	3	4	5	…	$n-3$	$n-2$	$n-1$	n
$n-3$	$n-2$	$n-1$	n	1	…	$n-7$	$n-6$	$n-5$	$n-4$

14. Зашифруйте с помощью открытого ключа (8051, 5) криптосистемы RSA сообщение m = 10.
    а) 8051.
    б) 3388.
    в) 1949.
    г) 12.
15. Какое свойство безопасности гарантирует, что участнику криптографического протокола целостности полученного сообщения и его создание до момента получения, но не гарантирует защиту от повторной отправки сообщения?
    а) Свойство «аутентификация сторон».
    б) Свойство «аутентификация источника».
    в) Свойство «инвариантность отправителя».
    г) Свойство «аутентификация сообщения».
16. Какое свойство безопасности гарантирует, что участнику криптографического протокола, что участники, начавшие исполнение протокола, не изменились с течением времени?
    а) Свойство «аутентификация сторон».
    б) Свойство «аутентификация источника».
    в) Свойство «инвариантность отправителя».
    г) Свойство «аутентификация сообщения».

Верный и полный ответ на вопрос теста оценивается в 1 балл, для прохождения теста необходимо верно и полно ответить на не менее чем 60 процентов вопросов теста.

Темы практических занятий

Тема практического занятия по теме 3.1
Введение в информационную безопасность операционных систем

1. Основы работы с процессами, вводом-выводом и файлами в ОС Windows и Linux.

Тема практического занятия по теме 3.2
Информационная безопасность операционных систем семейства Windows.

1. Основы обеспечения безопасности в ОС Windows.

Тема практического занятия по теме 3.3
Информационная безопасность операционных систем семейства Linux

1. Основы обеспечения безопасности в ОС Linux.

Тема практического занятия по теме 4.1
Введение в архитектуру локальных вычислительных сетей

1. Сетевой сниффер Wireshark. Знакомство с фильтрами пакетов.

Темы практического занятия по теме 4.2
Сетевые угрозы и методы противодействия им

1. Инвентаризация и поиск уязвимостей с использованием Open Vulnerability and Assessment Language.
2. Сетевой сканер Zenmap. Использование сетевого сканера для выявления уязвимостей уровня сети.
3. Вирусы, их выявление и устранение с использованием специализированного программного обеспечения.

Темы практического занятия по теме 4.3 Межсетевые экраны

1. Брандмауэр Windows. Разработка правил межсетевого экранирования.
2. Виртуальная инфраструктура Eve-NG.
3. Межсетевой экран на границе сети. Настройка правил межсетевого экранирования.

Темы практического занятия по теме 5.1
Введение в криптографические методы защиты информации

1. Исторические шифры шифрование и расшифрование.

Дополнительные задания для самостоятельного решения

Дополнительные задания по теме 1.1 Правовые основы обеспечения информационной безопасности

1. Какая информация представляет для Вас ценность? Какие характеристики информационной безопасности Вы бы хотели обеспечить для такой информации?
2. Выберете какой-либо вид ценной для Вас информации. В каких формах может быть представлен этот вид информации?
3. Проанализируйте: к каким видам тайн Вы можете иметь доступ?
4. Проанализируйте: какие связанные с Вами данные могут являться тайнами?

Дополнительные задания по теме 1.2 Защита персональных данных

1. Опишите схему информационных потоков Ваших персональных данных в Университете.
2. Опишите схему информационных потоков Ваших персональных данных в Банке.
3. Проанализируйте: всегда ли (когда это необходимо) с Вас взимают согласие на обработку персональных данных? Всегда ли это происходит в соответствии с законодательством?
4. Проанализируйте: в каких ситуациях Вы давали согласие на обработку Ваших специальных данных? Не было ли это излишним?
5. Проанализируйте: в каких ситуациях Вы давали согласие на обработку Ваших биометрических данных? Не было ли это излишним?

Дополнительные задания по теме 1.3 Организационные основы обеспечения информационной безопасности

1. Разработайте модель нарушителя для Вашей домашней информационной системы.
2. Разработайте модель нарушителя для компьютерного класса Университета.

3. Разработайте модель угроз для Вашей домашней информационной системы.
4. Разработайте модель нарушителя для компьютерного класса Университета.
5. Предложите средства защиты информации для Вашей домашней информационной системы.
6. Предложите средства защиты информации для компьютерного класса Университета.

Дополнительные задания по теме 2.1 Архитектура компьютера

1. Изучите Ваш персональный компьютер и современные гаджеты, которыми Вы пользуетесь. Сравните их характеристики: быстродействие, объем оперативной и вспомогательной памяти, скорость доступа в Интернет.

Дополнительные задания по теме 3.1 Введение в информационную безопасность операционных систем

ОС Windiws

1. Откройте браузер Internet Explorer. Найдите его идентификатор процесса, открытые соединения и базовый приоритет.
2. Откройте браузер Chrome. Найдите его идентификатор процесса, открытые соединения и базовый приоритет.
3. Запустите приложение «Блокнот». Найдите файлы открытые процессом «Блокнот» с помощью утилиты Process Explorer.

ОС Linux

1. Найдите пять самых требовательных к памяти процессов.
2. Откройте браузер и найдите открытые соединения.
3. Выведите содержимое директории /etc.
4. Выведите содержимое директории /etc/schedule.

Дополнительные задания по теме 3.2 Информационная безопасность операционных систем семейства Windows

1. Создайте пользователя «Алиса». Назначьте ей пароль. Создайте группу «Недоверенные пользователи».
2. Создайте директорию, содержащую файлы. Назначьте Алисе права достаточные для отображения списков файлов и переходов в директории и ее поддиректориях, а также чтения файлов в директории и ее поддиректориях. Проверьте, что Алиса может просматривать файлы.
3. Запретите группе «Недоверенные пользователи» любой доступ к созданной директории, ее поддиректориям, а также к файлам внутри директории и ее поддиректорий.
4. Добавьте Алису в группу «Недоверенные пользователи». Проверьте, что Алиса не сможет просматривать файлы в директории.

Дополнительные задания по теме 3.3 Информационная безопасность операционных систем семейства Linux

1. Создайте пользователя «Алиса». Назначьте ей пароль. Создайте группу «Недоверенные пользователи».

2. Создайте директорию, содержащую файлы. Назначьте Алисе права достаточные для отображения списков файлов и переходов в директории и ее поддиректориях, а также чтения файлов в директории и ее поддиректориях. Проверьте, что Алиса может читать файлы.
3. С помощью списка контроля доступов запретите группе «Недоверенные пользователи» любой доступ к выбранному файлу внутри директории. Поменяйте владельца этого файла на суперпользователя системы. Разрешите в базовых правах доступ к выбранному файлу кодом 600.
4. Добавьте Алису группу «Недоверенные пользователи». Проверьте, что Алиса не сможет прочитать выбранный файл.

Дополнительные задания по теме 4.1 Введение в архитектуру локальных вычислительных сетей

1. Проверьте доступность любого используемого Вами почтового сервера с использованием утилиты Telnet. Следуйте статье https://docs.microsoft.com/ru-ru/exchange/mail-flow/test-smtp-with-telnet?view=exchserver-2019 и самостоятельно.
2. Настройте почту в почтовом клиенте Thunderbird. Следуйте статье https://support.mozilla.org/ru/kb/nastrojki-konfiguracii-dlya-uchyotnyh-zapisej.
3. Разработайте фильтры для просмотра только исходящих ICMP-запросов. Следуйте статье https://habr.com/ru/post/211042/.

Дополнительные задания по теме 4.2 Сетевые угрозы и методы противодействия им

1. Проведите поиск уязвимостей на своем домашнем персональном компьютере, ознакомьтесь с описанием выявленных уязвимостей, определите насколько они критичны по шкале CVSS, и устраните их.
2. Проверьте, устранена ли уязвимость CVE-2017-0144 на вашем домашнем компьютере, и установите обновление безопасности в случае, если уязвимость присутствует. Следуйте статье https://support.microsoft.com/ru-ru/help/4023262/how-to-verify-that-ms17-010-is-installed.
3. Изучите уязвимость CVE-2014-0160, следуя статьям https://xkcd.ru/1354/ http://mirror3.esetnod32.ru/company/virlab/analytics/2014-05-05-ujazvimost-heartbleed.pdf. Первая статья представляет собой небольшой комикс, показывающий, насколько опасна и легко используема эта уязвимость. Вторая статья представляет собой подробное описание уязвимости, последствия ее использования и риски.

Дополнительные задания по теме 4.3 Межсетевые экраны

1. Замените узлы Hacker и Victim на узлы под управлением операционной системы Windows и обратитесь к их сетевым ресурсам по протоколу SMB. Следуйте статье https://www.eve-ng.net/index.php/documentation/howtos/howto-create-own-windows-host-on-the-eve/.

Дополнительные задания по теме 5.1 Введение в криптографические методы защиты информации

1. Зашифруйте и расшифруйте сообщение «Я тебя люблю!» всеми известными Вам историческими шифрами.

Критерии оценки практического занятия.

За практическое задание выполняется одна из оценок: «**отлично**», «**хорошо**», «**удовлетворительно**», «**неудовлетворительно**».

Оценка «отлично» выставляется, если студент активно работает в течение всего практического занятия, дает верные и полные ответы на вопросы преподавателя и показывает при этом глубокое овладение лекционным материалом, все части задания выполнены верно (допускаются небольшие неточности, не являющиеся следствием незнания или непонимания учебного материала). Работа выполнена самостоятельно. Работа сдана с соблюдением всех сроков. Соблюдены все правила оформления.

Оценка «хорошо» выставляется, если студент активно работает в течение всего практического занятия, дает верные, но возможно неполные ответы на вопросы преподавателя и показывает при этом свободное владение лекционным материалом, все части задания выполнены верно (допускаются неточности, не являющиеся следствием незнания или непонимания учебного материала). Работа в целом выполнена самостоятельно, возможно с консультацией преподавателя. Работа сдана с соблюдением всех сроков. Допускаются незначительные недочеты в оформлении.

Оценка «удовлетворительно» выставляется в том случае, когда студент в целом овладел сутью вопросов по данной теме, обнаруживает знание лекционного материала. При этом на занятии ведет себя пассивно, дает неполные ответы на вопросы, допускает ошибки при освещении теоретического материала, не может обобщить и сделать четкие логические выводы. Работа сдана с опозданием не более двух занятий. Допускаются незначительные недочеты в оформлении.

Оценка «неудовлетворительно» выставляется в случае, когда студент обнаружил несостоятельность осветить вопросы или вопросы освещены неправильно, бессистемно, с грубыми ошибками, отсутствуют понимания основной сути вопросов, выводы, обобщения, обнаружено неумение решать учебные задачи. Обучающийся не может выполнить работу без помощи преподавателя. Работа сдана с нарушением сроков (позднее чем через два занятия). В оформлении присутствуют значительные недочеты.

1.2 Список вопросов и (или) заданий для проведения промежуточной аттестации

Вопросы к зачету

1. Основные права граждан в сфере обработки и защиты информации.
2. Основные принципы правового регулирования в области обработки и защиты информации.
3. Информация. Основные свойства безопасности информации: конфиденциальность, целостность, доступность.
4. Виды информации по порядку доступа и распространения.
5. Ограничение доступа к информации. Защита информации. Объекты защиты. Виды тайн.
6. Информационные технологии и информационные системы.
7. Обладатель информации и оператор информационной системы.
8. Ответственность в сфере обработки и защиты информации.
9. Персональные данные и принципы их обработки.
10. Виды персональных данных: специальные, биометрические и общедоступные.
11. Условия обработки персональных данных.
12. Согласие на обработку персональных данных.
13. Трансграничная передача персональных данных.

14. Права субъектов персональных данных.
15. Оператор персональных данных и его обязанности.
16. Меры обеспечения безопасности персональных данных.
17. Контроль и надзор за выполнением мер по обеспечению безопасности.
18. Уполномоченный орган по защите прав субъектов персональных данных.
19. Последовательность действий по защите информации.
20. Выявление и анализ информационных активов.
21. Формирование требований по защите информации.
22. Подходы к моделированию нарушителей информационной безопасности.
23. Угрозы информационной безопасности.
24. Средства защиты информации.
25. Процессоры.
26. Основная (кэш и оперативная) память.
27. Вспомогательная память.
28. Устройства ввода-вывода (шины, мониторы, принтеры).
29. Устройства ввода-вывода (клавиатуры и мыши, веб-камеры, микрофоны).
30. Общий способ хранения и обработки информации в компьютере.
31. Понятия операционной и файловой систем.
32. Субъекты, объекты, методы и права доступа, привилегии субъекта доступа.
33. Дискреционное управление доступом.
34. Мандатное управление доступом.
35. Идентификация, аутентификация и авторизация.
36. Управление доступом в операционных системах семейства Windows.
37. Идентификация, аутентификация и авторизация в операционных системах семейства Windows.
38. Реализация аудита в операционных системах семейства Windows.
39. Управление доступом в операционных системах семейства Linux.
40. Идентификация, аутентификация и авторизация в операционных системах семейства Linux.
41. Модель ISO/OSI.
42. Архитектура и основные протоколы локальных вычислительных сетей.
43. Классификации сетевых угроз, уязвимостей и атак.
44. Сетевые атаки на различных уровнях модели ISO/OSI.
45. Классификация вредоносного программного обеспечения.
46. Признаки присутствия вредоносного программного обеспечения.
47. Методы обнаружения вредоносного программного обеспечения.
48. Место и роль межсетевых экранов в обеспечении сетевой безопасности.
49. Классификация межсетевых экранов.
50. Основные возможности межсетевых экранов.
51. Достоинства и недостатки межсетевых экранов.
52. Построение правил фильтрации.
53. Криптография древнего мира.
54. Криптография средних веков.
55. Криптография эпохи Возрождения.
56. Криптография Нового времени.
57. Симметричная и асимметричная криптография.
58. Вычислительно сложные задачи математики.
59. Криптосистема RSA.
60. Понятие криптографического протокола.
61. Свойства протоколов, характеризующие их безопасность.
62. Схемы цифровой подписи.

Правила выставления оценки на зачете.

В процессе зачета требуется ответить на один из приведенных выше вопросов. На подготовку к ответу дается не менее 1 академического часа.

По итогам зачета выставляется одна из оценок: «зачтено», «не зачтено».

Оценка «Зачтено» выставляется студенту, который демонстрирует **в**ладение содержанием материала и понятийным аппаратом теории псевдослучайных генераторов; умеет связывать теорию с практикой. В ответе могут допускаться отдельные неточности (несущественные ошибки), которые исправляются самим студентом после дополнительных и (или) уточняющих вопросов экзаменатора. На часть дополнительных вопросов студент может не дать ответ или дать неверный ответ.

Оценка «Не зачтено» выставляется студенту, который демонстрирует разрозненные, бессистемные знания; беспорядочно и неуверенно излагает материал; не умеет выделять главное и второстепенное, не умеет соединять теоретические положения с практикой; допускает грубые ошибки при определении понятий, вследствие непонимания их существенных и несущественных признаков и связей; дает неполные ответы, логика и последовательность изложения которых имеют существенные и принципиальные нарушения, в ответах отсутствуют выводы. Дополнительные и уточняющие вопросы экзаменатора не приводят к коррекции ответов студента. На основную часть дополнительных вопросов студент затрудняется дать ответ или дает неверные ответы.

Оценка «Не зачтено» выставляется также студенту, который взял экзаменационный билет, но отказался дать на него ответ.

Приложение №2 к рабочей программе дисциплины
«Безопасность в современной информационной среде»

Методические указания для обучающихся по освоению дисциплины

Основной формой изложения учебного материала по дисциплине «Безопасность в современной информационной среде» являются лекции, что связано, прежде всего, с новизной материала для обучающихся. По большинству тем предусмотрены практические занятия, целью которых является закрепление лекционного материала путем решения специальным образом подобранных практических задач.

Для успешного освоения дисциплины важно самостоятельное изучение теоретического материала и решение практических задач, как в аудитории, так и самостоятельно в качестве самостоятельной работы. Примеры решения задач разбираются на лекциях и практических занятиях, при необходимости по наиболее трудным темам проводятся дополнительные консультации. Основная цель решения практических задач – помочь усвоить основные понятия информационной безопасности, их определения, а также основные методы и средства обеспечения информационной безопасности. Для решения задач необходимо не только знать, но и понимать лекционный материал. Поэтому в процессе изучения дисциплины рекомендуется регулярная работа с конспектами лекций и рекомендованной литературой.

Большое внимание должно быть уделено самостоятельной работе. В качестве заданий для самостоятельной работы дома студентам предлагаются задачи, аналогичные разобранным на лекциях и практических занятиях или схожие с ними.

Для проверки и контроля усвоения теоретического материала, приобретенных практических навыков работы с основными понятиями в течение обучения проводятся мероприятия текущей аттестации в виде тестирований. Также проводятся консультации (при необходимости) по лекционному материалу и разбору некоторых заданий для самостоятельной работы.

В конце изучения дисциплины студенты сдают зачет. Зачет проводится на основании выполнения тестовых заданий и собеседования на основании списка вопросов к зачету, который охватывает полностью всю программу дисциплины.

Учебно-методическое обеспечение самостоятельной работы студентов по дисциплине

Для самостоятельной работы рекомендуется использовать следующую учебную литературу:

1. Таненбаум Э. Архитектура компьютера. / Э. Таненбаум; [пер. с англ. Ю. Гороховского, Д. Шинтякова] - 5-е изд. - СПб.: Питер, 2013. - 843 с. (академическое изложение материала по архитектуре компьютера).
2. Таненбаум Э. Современные операционные системы. / Э. Таненбаум, Х. Бос; [пер. с англ. А. Леонтьевой, М. Малышевой, Н. Вильчинского] - 4-е изд. - СПб.: Питер, 2019. - 1119 с.: ил. (академическое изложение материала по операционным системам).
3. Таненбаум Э. Компьютерные сети. / Э. Таненбаум, Д. Уэзеролл; [пер. с англ. А. Гребенькова] - 5-е изд. - СПб.: Питер, 2019. - 955 с. (академическое изложение материала по компьютерным сетям).
4. Алферов А.П. Основы криптографии. Учебное пособие. / А.П. Алферов, А. Ю. Зубов, А.С. Кузьмин, А.В. Черемушкин. М.: Гелиос АРВ, 2005. 480 с. (академическое изложение материала по криптографии).