МИНИСТЕРСТВО НАУКИ И ВЫСШЕГО ОБРАЗОВАНИЯ
РОССИЙСКОЙ ФЕДЕРАЦИИ

Федеральное государственное бюджетное образовательное учреждение высшего образования
«Луганский государственный университет имени Владимира Даля»

Экономический факультет
Кафедра экономической кибернетики и прикладной статистики

УТВЕРЖДАЮ:
Декан
Экономического факультета
_____ Тхор Е.С.
(подпись)
« 24 » апреля 2023 года

РАБОЧАЯ ПРОГРАММА УЧЕБНОЙ ДИСЦИПЛИНЫ

«ИНФОРМАЦИОННАЯ БЕЗОПАСНОСТЬ ЭКОНОМИЧЕСКОЙ ДЕЯТЕЛЬНОСТИ»

Направление подготовки 38.05.01 Экономическая безопасность
Специализация «Экономика и организация производства на режимных объектах»

Луганск – 2023

Лист согласования РПУД

Рабочая программа учебной дисциплины «Информационная безопасность экономической деятельности» по направлению подготовки 38.05.01 Экономическая безопасность. – 48 с.

Рабочая программа учебной дисциплины «Информационная безопасность экономической деятельности» составлена с учетом Федерального государственного образовательного стандарта высшего образования по направлению подготовки 38.05.01 Экономическая безопасность Министерства науки и высшего образования Российской Федерации от 14 апреля 2021 года № 293.

СОСТАВИТЕЛЬ:
к.э.н., доцент Воронова А.Г.

Рабочая программа дисциплины утверждена на заседании кафедры экономической кибернетики и прикладной статистики «18» 04 2023 г., протокол № 26

Заведующий кафедрой
экономической кибернетики и прикладной статистики _____ Велигура А.В.

Переутверждена: «___» _____20___ г., протокол № _____

Согласована (для обеспечивающей кафедры):
Заведующий кафедрой менеджмента и экономической безопасности
_____ Тисунова В.Н.
Переутверждена: «___» _____20____ года, протокол № _____

Рекомендована на заседании учебно-методической комиссии экономического факультета «21» апреля 2023 г., протокол № 4.

Председатель учебно-методической
комиссии института _____ _____ Е.Н. Шаповалова

Структура и содержание дисциплины

1. Цели и задачи дисциплины, ее место в учебном процессе

Цель изучения дисциплины – приобретение студентами теоретических знаний и практических знаний и навыков защиты информации, потенциальных угрозах и проблемах защиты данных в локальных системах и компьютерных сетях.

Задачами дисциплины является получение знания об общих сведения по защите информации, классификации угроз информации современных средств, методов и технологий обеспечения информационной безопасности, в том числе получение знаний об основных криптографических процедурах для обеспечения аутентичности, целостности и конфиденциальности информации.

2. Место дисциплины в структуре ООП ВО

Дисциплина "Информационная безопасность экономической деятельности" относится к циклу обязательных дисциплин.

Необходимыми условиями для освоения дисциплины являются:

знания:

- основные стандарты в области информационной безопасности;
- основные положения законодательства в области защиты информации;
- возможные уязвимости и угрозы воздействия нарушителей;
- основные инструментальные средства защиты информации;
- принципы криптоанализа;
- организационную и правовую ответственности за утечку защищаемой информации и потерю ее носителей;

умения:

- анализировать и оценивать уязвимости и угрозы информационной безопасности объекта;
- формулировать соответствующие требования к системам защиты информации;
- обеспечивать грамотный подбор программно-аппаратных и программных средств для обеспечения необходимого уровня защиты информации;
- осуществлять меры противодействия нарушениям информационной безопасности с использованием различных программных и аппаратных средств защиты;

навыки:

- базовыми навыками построения и управления систем защиты информации;
- методами и средствами выявления угроз безопасности автоматизированным системам;
- навыками применения штатных средств защиты информации;
- навыками решения задач криптоанализа и шифрования.

Содержание дисциплины является логическим продолжением содержания дисциплин «Введение в специальность», «Бизнес-информатика», «Основы национальной безопасности» и служит основой для освоения дисциплин «Информационные системы и технологии в управленческой деятельности», «Обеспечение экономической безопасности хозяйствующего субъекта» практик студентов.

3. Требования к результатам освоения содержания дисциплины

Код и наименование компетенции	Индикаторы достижений компетенции (по реализуемой дисциплине)	Перечень планируемых результатов
ОПК-6. Способен использовать современные информационные технологии и программные средства при решении профессиональных задач	ОПК-6.1. Демонстрирует знание информационных технологий и программных средств, в том числе отечественного производства, применяемых предприятиями для решения задач обеспечения экономической безопасности на современном этапе ОПК-6.2. Выбирает и применяет современные информационные технологии и программные средства для решения профессиональных задач экономической безопасности хозяйствующего субъекта	Знать: – основные инструментальные средства защиты информации; Уметь: – обеспечивать грамотный подбор программно-аппаратных и программных средств для обеспечения необходимого уровня защиты информации; Владеть: – навыками применения штатных средств защиты информации; – навыками решения задач криптоанализа и шифрования.
ОПК-7. Способен понимать принципы работы современных информационных технологий и использовать их для решения задач профессиональной деятельности	ОПК-7.1. Знает и понимает принципы работы и возможности современных информационных технологий, предназначенных для решения задач обеспечения экономической безопасности ОПК-7.2. Использует современные информационные технологии для решения задач профессиональной деятельности	Знать: – основные стандарты в области информационной безопасности; – основные положения законодательства в области защиты информации; – возможные уязвимости и угрозы воздействия нарушителей; – принципы криптоанализа; Уметь: – анализировать и оценивать уязвимости и угрозы информационной безопасности объекта; – формулировать соответствующие требования к системам

		защиты информации;
		Владеть: – базовыми навыками построения и управления систем защиты информации; – методами и средствами выявления угроз безопасности автоматизированным системам;

4. Структура и содержание дисциплины

4.1. Объем учебной дисциплины и виды учебной работы

Вид учебной работы	Объем часов (зач. ед.)		
	Очная форма	**Очно-заочная форма**	**Заочная форма**
Общая учебная нагрузка (всего)	**144 (4 зач. ед)**		**144 (4 зач. ед)**
Обязательная контактная работа (всего) в том числе:	**54**		**14**
Лекции	18		4
Семинарские занятия	-		-
Практические занятия	36		10
Лабораторные работы	-		-
Курсовая работа (курсовой проект)	-		-
Другие формы и методы организации образовательного процесса (*расчетно-графические работы,* индивидуальные задания *и т.п.)*	-		-
Самостоятельная работа студента (всего)	**90**		**130**
Форма аттестации	экзамен		экзамен

4.2. Содержание разделов дисциплины

Тема 1. ВВЕДЕНИЕ В ДИСЦИПЛИНУ "ИНФОРМАЦИОННАЯ БЕЗОПАСНОСТЬ ЭКОНОМИЧЕСКОЙ ДЕЯТЕЛЬНОСТИ"

Цель и задачи дисциплины, ее роль и место в общей системе подготовки специалиста. Понятие информационной безопасности. Важность и сложность проблемы информационной безопасности. Место информационной безопасности экономических систем в национальной безопасности страны. Основные составляющие информационной безопасности.

Тема 2. ЗАКОНОДАТЕЛЬНАЯ ОСНОВА ИНФОРМАЦИОННОЙ БЕЗОПАСНОСТИ

Основные положения нормативной базы РФ и национальных стандартов в области информационной безопасности и защиты информации. Современное состояние компьютерной преступности и ответственность за нарушения и преступления в сфере информационной безопасности. Информационная безопасность на уровне государства и предприятия.

Тема 3. УГРОЗЫ ИНФОРМАЦИОННОЙ БЕЗОПАСНОСТИ

Ключевые аспекты и вопросы формирования информационной безопасности (ИБ) современного предприятия. Уровни и структура ИБ. Основные определения и критерии классификации угроз. Основные угрозы безопасности ИТ-инфраструктуры современного предприятия. Каналы силового деструктивного воздействия на информацию. Технические каналы утечки информации. Угрозы несанкционированного доступа к информации. Нетрадиционные информационные каналы. Вирусы как особый класс разрушающих программных действий.

Тема 4. ПРОГРАММНО-ТЕХНИЧЕСКИЕ МЕТОДЫ И СРЕДСТВА ЗАЩИТЫ ИНФОРМАЦИИ

Правовые, программно-технические и организационно-экономические методы защиты информации. Направления развития методов и средств защиты информации при ее обработке в информационных системах.

Методы и средства разграничения и контроля доступа к информации. Матричный и мандатный подходы к организации разграничения прав доступа к информации. Права доступа в Windows и Linux.

Понятие об идентификации пользователя и его особенности. Основные принципы и методы аутентификации. Одноразовые пароли. Идентификация и аутентификация с помощью биометрических данных. Организационные требования. Требования к документированию. Протоколирование, тестирование программ и обработка угроз.

Методы хранения данных. RAID массивы. Сохранение данных на скрытых разделах. Шифрование скрытого раздела жесткого диска. Резервное копирование: инкрементное, дифференциальное, полное.

Системы предотвращения утечки информации из корпоративной сети.

Тема 5. КРИПТОГРАФИЧЕСКИЕ МЕХАНИЗМЫ ЗАЩИТЫ ИНФОРМАЦИИ В ИНФОРМАЦИОННЫХ СИСТЕМАХ

Криптографическая защита информации. Симметричные криптосистемы. Криптосистемы с открытым ключом. Цифровая подпись. Требования к цифровой подписи. Правовые аспекты использования цифровой подписи. Криптосистема шифрования данных RSA.

Тема 6. МЕТОДЫ КРИПТОГРАФИЧЕСКОГО ЗАКРЫТИЯ ИНФОРМАЦИИ. ШИФРОВАНИЕ. КОДИРОВАНИЕ

Классификация основных методов криптографического закрытия информации. Шифрование: Подстановка (замена). Перестановка (по методу Гамильтона). Гаммирование. Аналитические преобразования. Комбинированные методы шифрования.

Тема 7. МЕТОДЫ КОДИРОВАНИЯ ИНФОРМАЦИИ.

Символьное кодирования. Смысловое кодирование Метод "Стопка книг", Метод Савчука, Одноалфавитное и многоалфавитное смысловое кодирование.

Метод рассечения-разнесения данных: механическое и смысловое.

Тема 8. МЕТОДЫ СЖАТИЯ-РАСШИРЕНИЯ ИНФОРМАЦИИ.

Метод Хаффмана (Дерево Хаффмана). Арифметический код. Zip-модификация алгоритма Лемпеля-Зива. LZW-модификация алгоритма Лемпеля-Зива.

Тема 9. УПРАВЛЕНИЕ ИНФОРМАЦИОННОЙ БЕЗОПАСНОСТЬЮ

Методология решения задач управления информационной безопасностью. Модели и методы реализации системы обеспечения информационной безопасности. Управление обновлениями программных средств. Управление конфигурациями. Разграничение доступа к сетевому оборудованию. Архитектура управления информационной безопасностью. Мониторинг и аудит безопасности информационной системы.

4.3. Лекции

№ п/п	Название темы	Объем часов		
		Очная форма	Очно-заочная форма	Заочная форма
1.	Тема 1. Введение в дисциплину "Информационная безопасность экономической деятельности"	2		0,4
2.	Тема 2. Законодательная основа информационной безопасности	2		0,4
3.	Тема 3. Угрозы информационной безопасности	2		0,4
4.	Тема 4. Программно-технические методы и средства защиты информации.	2		0,8
5.	Тема 5. Криптографические механизмы защиты информации в информационных системах	2		0,4
6.	Тема 6. Методы криптографического закрытия информации. Шифрование	2		0,4
7.	Тема 7. Методы кодирования информации	2		0,4
8.	Тема 8. Методы сжатия-расширения информации	2		0,4
9.	Тема 9. Управление информационной безопасностью	2		0,4
Итого:		**18**		**4**

4.4. Практические (семинарские) занятия

№ п/п	Название темы	Объем часов		
		Очная форма	Очно-заочная форма	Заочная форма
1.	RSA-шифрование	4		1
2.	Перестановка (по методу Гамильтона).	2		1
3.	Гаммирование.	4		1
4.	Метод "Стопка книг". Метод Савчука.	4		1
5.	Метод Хаффмана (Дерево Хаффмана). Арифметический код.	4		1
6.	Метод рассечения-разнесения данных	4		1

7.	Zip-модификация алгоритма Лемпеля-Зива. LZW-модификация алгоритма Лемпеля-Зива.	4		1
8.	Парольная защита документов. Расчет стойкости пароля	2		1
9.	Электронная цифровая подпись	4		1
10.	Анализ рисков информационной безопасности. CORAS	4		1
Итого:		**36**		**10**

4.6. Самостоятельная работа студентов

№ п/п	Название темы	Вид СРС	Объем часов		
			Очная форма	Очно-заочная форма	Заочная форма
1.	RSA-шифрование	самостоятельное изучение темы дисциплины	5		10
2.	Перестановка (по методу Гамильтона).	самостоятельное изучение темы дисциплины	5		8
3.	Гаммирование.	самостоятельное изучение темы дисциплины	5		8
4.	Метод "Стопка книг". Метод Савчука.	самостоятельное изучение темы дисциплины	5		8
5.	Метод Хаффмана (Дерево Хаффмана). Арифметический код.	самостоятельное изучение темы дисциплины	5		8
6.	Метод рассечения-разнесения данных	самостоятельное изучение темы дисциплины	5		12
7.	Zip-модификация алгоритма Лемпеля-Зива. LZW-модификация алгоритма Лемпеля-Зива.	самостоятельное изучение темы дисциплины	5		8
8.	Парольная защита документов. Расчет стойкости пароля	самостоятельное изучение темы дисциплины	5		8
9.	Электронная цифровая подпись	самостоятельное изучение темы дисциплины	4		8
10.	Анализ рисков информационной безопасности. CORAS	самостоятельное изучение темы дисциплины	10		16
11.	Подготовка к зачету/экзамену	Повтор теоретического материалы.	36		36
Итого:			**90**		**130**

4.7. Курсовые работы/проекты по дисциплине «Информационная безопасность экономической деятельности» не предполагаются учебным планом.

5. Образовательные технологии

Преподавание дисциплины ведется с применением следующих видов образовательных технологий: объяснительно-иллюстративного обучения (технология поддерживающего обучения, технология проведения учебной дискуссии), информационных технологий (презентационные материалы), развивающих и инновационных образовательных технологий.

Практические занятия проводятся с использованием развивающих, проблемных, проектных, информационных (использование электронных образовательных ресурсов (электронный конспект) образовательных технологий.

6. Учебно-методическое и информационное обеспечение дисциплины:

а) основная литература:

1. Майорова, Е. В. Организационное и правовое обеспечение информационной безопасности : Учебное пособие / Е. В. Майорова, А. М. Полегенько. – Санкт-Петербург : Санкт-Петербургский государственный экономический университет, 2020. – 87 с. – ISBN 978-5-7310-5332-7. – EDN CRFFYY. — URL : https://www.elibrary.ru/download/elibrary_46174849_62120187.pdf
2. Сухостат, В. В. Информационная безопасность : Учебное пособие / В. В. Сухостат. – Санкт-Петербург : Санкт-Петербургский государственный экономический университет, 2021. – 98 с. – ISBN 978-5-7310-5584-0. – EDN THDMKU. — URL : https://www.elibrary.ru/download/elibrary_48073406_35238015.pdf
3. Информационная безопасность : Учебное пособие предназначено для освоения дисциплин Информационная безопасность, Защита информации для обучающихся по направлениям подготовки Информационные системы и технологии, Прикладная информатика / В. И. Лойко, С. В. Лаптев, В. Н. Лаптев, Г. А. Аршинов. – Краснодар : Кубанский государственный аграрный университет имени И.Т. Трубилина, 2020. – 332 с. – ISBN 978-5-907346-50-5. – EDN FWFFBG. — URL : https://www.elibrary.ru/download/elibrary_45486035_15164620.PDF
4. Бабенко, Л. К. Криптографическая защита информации: симметричное шифрование : учебное пособие / Л. К. Бабенко, Е. А. Ищукова ; ЮЖНЫЙ ФЕДЕРАЛЬНЫЙ УНИВЕРСИТЕТ. – Таганрог : Издательство Южного федерального университета, 2015. – 219 с. – EDN VIUWIP. — URL : https://www.elibrary.ru/download/elibrary_25353132_85779244.pdf

б) дополнительная литература:

1. Груздева, Л. М. Информационная безопасность : Учебно-методическое пособие / Л. М. Груздева ; Российский университет транспорта (МИИТ). – Москва : Издательский Дом "Академия Естествознания", 2020. – 121 с. – ISBN 978-5-91327-662-9. – DOI 10.17513/np.432. – EDN ZYAAJZ. — URL : https://www.elibrary.ru/download/elibrary_44668615_93844582.pdf
2. Платонов, А. А. Информационная безопасность : Учебное пособие [Электронный ресурс] / А. А. Платонов. – Волгоград : Волгоградский государственный архитектурно-строительный университет, 2016. – 69 с. – ISBN 978-5-98276-822-3. – EDN YIGINP. — URL : https://www.elibrary.ru/download/elibrary_28892005_89625832.pdf
3. Терелянский, П. В. Информационная безопасность : учебное пособие / П. В. Терелянский, И. А. Тарасова, Т. С. Фролова. – Волгоград : Волгоградский государственный технический университет, 2015. – 96 с. – ISBN 978-5-9948-2004-9. – EDN VFYWNT. — URL : https://www.elibrary.ru/download/elibrary_25223083_76817147.pdf
4. Макаренко, С. И. Информационная безопасность: учебное пособие : учебное пособие / С. И. Макаренко. – Ставрополь, 2009. – 372 с. – EDN QIRWUL. . — URL : https://www.elibrary.ru/download/elibrary_19407202_92560555.pdf
5. Васильева, И. Н. Управление информационной безопасностью : учебное пособие / И. Н. Васильева ; Санкт-Петербургский государственный экономический университет. – Санкт-Петербург : Санкт-Петербургский государственный экономический университет, 2014. – 82 с. – EDN TCMFPV. — URL : https://www.elibrary.ru/download/elibrary_22687480_14258248.pdf
6. Васильева, И. Н. Управление рисками информационной безопасности / И. Н. Васильева. – Санкт-Петербург : Санкт-Петербургский государственный экономический университет, 2016. – 177 с. – ISBN 978-5-7310-3817-1. – EDN ZQUEHR. — URL : https://www.elibrary.ru/download/elibrary_30470044_25031716.pdf
7. Майорова, Е. В. Организационное и правовое обеспечение информационной безопасности : Учебное пособие / Е. В. Майорова, А. М. Полегенько. – Санкт-Петербург : Санкт-Петербургский государственный экономический университет, 2020. – 87 с. – ISBN 978-5-7310-5332-7. – EDN CRFFYY. — URL : https://www.elibrary.ru/download/elibrary_46174849_62120187.pdf
8. Закон РФ от 21.07.1993 N 5485-1 (ред. от 08.03.2015) "О государственной тайне"
9. Федеральный закон от 27.07.2006 N 149-ФЗ (ред. от 19.12.2016) "Об информации, информационных технологиях и о защите информации"

в) методические рекомендации:

1. Конспект лекций по дисциплине «Обеспечение надежности и безопасности экономических информационных систем» для студентов направления подготовки 38.03.05 – Бизнес-информатика (дневной и заочной форм обучения) / Сост.: А.Г. Воронова. – Луганск: изд-во ЛНУ им. В. Даля, 2018. – 102 с.

2. Методические указания к практическим занятиям по дисциплине «Обеспечение надежности и безопасности экономических информационных систем» для студентов направления подготовки 38.03.05 – Бизнес-информатика (дневной и заочной форм обучения) / Сост.: А.Г. Воронова. – Луганск: изд-во: ЛНУ им. В. Даля, 2018. – 77 с.

3. Методические указания к практическим занятиям по дисциплине «Информационная безопасность» для студентов направления подготовки 38.03.04 Государственное и муниципальное управление (дневной и заочной форм обучения) / Сост.: А.Г. Воронова. – Луганск: изд-во: ЛГУ им. В. Даля, 2023. – 113 с.

г) Интернет-ресурсы:

Министерство образования и науки Российской Федерации – http://минобрнауки.рф/

Федеральная служба по надзору в сфере образования и науки – http://obrnadzor.gov.ru/

Портал Федеральных государственных образовательных стандартов высшего образования – http://fgosvo.ru

Федеральный портал «Российское образование» – http://www.edu.ru/

Информационная система «Единое окно доступа к образовательным ресурсам» – http://window.edu.ru/

Федеральный центр информационно-образовательных ресурсов – http://fcior.edu.ru/

Справочно-правовая система «Консультант плюс». - URL: http://base.consultant.ru

Научная электронная библиотека. - URL: http://elibrary.ru/

Электронные библиотечные системы и ресурсы

Электронно-библиотечная система «StudMed.ru» – https://www.studmed.ru

Информационный ресурс библиотеки образовательной организации

Научная библиотека имени А. Н. Коняева – http://biblio.dahluniver.ru/

7. Материально-техническое и программное обеспечение дисциплины

Освоение дисциплины «Информационная безопасность экономической деятельности» предполагает использование академических аудиторий, соответствующих действующим санитарным и противопожарным правилам и нормам.

Прочее: рабочее место преподавателя, оснащенное компьютером с доступом в Интернет.

Программное обеспечение:

Функциональное назначение	**Бесплатное программное обеспечение**	**Ссылки**
Офисный пакет	Libre Office 6.3.1	https://www.libreoffice.org/ https://ru.wikipedia.org/wiki/LibreOffice
Операционная система	UBUNTU 19.04	https://ubuntu.com/ https://ru.wikipedia.org/wiki/Ubuntu
Браузер	Firefox Mozilla	http://www.mozilla.org/ru/firefox/fx
Браузер	Opera	http://www.opera.com
Почтовый клиент	Mozilla Thunderbird	http://www.mozilla.org/ru/thunderbird
Файл-менеджер	Far Manager	http://www.farmanager.com/download.php
Архиватор	7Zip	http://www.7-zip.org/
Графический редактор	GIMP (GNU Image Manipulation Program)	http://www.gimp.org/ http://gimp.ru/viewpage.php?page_id=8 http://ru.wikipedia.org/wiki/GIMP
Редактор PDF	PDFCreator	http://www.pdfforge.org/pdfcreator
Аудиоплейер	VLC	http://www.videolan.org/vlc/

8. Оценочные средства по дисциплине

Паспорт
фонда оценочных средств по учебной дисциплине
«Информационная безопасность экономической деятельности»

Перечень компетенций (элементов компетенций), формируемых в результате освоения учебной дисциплины (модуля) или практики

№ п/п	Код контролируемой компетенции	Формулировка контролируемой компетенции	Индикаторы достижений компетенции (по реализуемой дисциплине)	Контролируемые темы учебной дисциплины, практики	Этапы формирования (семестр изучения)
1	ОПК-6	Способен использовать современные информационные технологии и программные средства при решении профессиональных задач	ОПК-6.1. Демонстрирует знание информационных технологий и программных средств, в том числе отечественного производства, применяемых предприятиями для решения задач обеспечения экономической безопасности на современном этапе ОПК-6.2. Выбирает и применяет современные информационные технологии и программные средства для решения профессиональных задач экономической безопасности хозяйствующего субъекта	Тема 4. Программно-технические методы и средства защиты информации.	6
				Тема 5. Криптографические механизмы защиты информации в информационных системах	6
				Тема 6. Методы криптографического закрытия информации. Шифрование	6
				Тема 7. Методы кодирования информации	6
				Тема 8. Методы сжатия-расширения информации	6

2.	ОПК-7	Способен понимать принципы работы современных информационных технологий и использовать их для решения задач профессиональной деятельности	ОПК-7.1. Знает и понимает принципы работы и возможности современных информационных технологий, предназначенных для решения задач обеспечения экономической безопасности ОПК-7.2. Использует современные информационные технологии для решения задач профессиональной деятельности	Тема 1. Введение в дисциплину "Информационная безопасность"	6
				Тема 2. Законодательная основа информационной безопасности	6
				Тема 3. Угрозы информационной безопасности	6
				Тема 4. Программно-технические методы и средства защиты информации.	6
				Тема 9. Управление информационной безопасностью	6

Показатели и критерии оценивания компетенций, описание шкал оценивания

№ п/п	Код контролируемой компетенции	Индикаторы достижений компетенции (по реализуемой дисциплине	Перечень планируемых результатов	Контролируемые темы учебной дисциплины	Наименование оценочного средства
1.	ОПК-6	ОПК-6.1 ОПК-6.2	знать: основные инструментальные средства защиты информации уметь: обеспечивать грамотный подбор программно-аппаратных и	Тема 4-8	Устный опрос, задания (по вариантам)

			программных средств для обеспечения необходимого уровня защиты информации; владеть: навыками применения штатных средств защиты информации; навыками решения задач криптоанализа и шифрования.		
2.	ОПК-7	ОПК-7.1 ОПК-7.2	знать основные стандарты в области информационной безопасности; основные положения законодательства в области защиты информации; возможные уязвимости и угрозы воздействия нарушителей; принципы криптоанализа уметь анализировать и оценивать уязвимости и угрозы информационной безопасности объекта; формулировать соответствующие требования к системам защиты информации; владеть: базовыми навыками построения и управления систем защиты информации;	Тема 1-4, Тема 9	Устный опрос, задания (по вариантам)

			методами и средствами выявления угроз безопасности автоматизированным системам;		

Фонды оценочных средств по дисциплине «Информационная безопасность экономической деятельности»

Вопросы для обсуждения на практических и семинарских занятиях (устный опрос)

1. Понятие информационной безопасности.
2. Виды защищаемой информации.
3. Типы атак и угроз.
4. Внешние источники угроз
5. Внутренние источники угроз
6. Каналы утечки информации.
7. Стандарты информационной безопасности.
8. Основные методы обеспечения информационной безопасности.
9. Принципы построения защищенных систем.
10. Симметричные криптосистемы.
11. Ассиметричные криптосистемы.
12. RSA шифрование
13. Перестановка (по методу Гамильтона).
14. Гаммирование.
15. Аналитические преобразования.
16. Метод "Стопка книг". Метод Савчука.
17. Метод рассечения-разнесения данных
18. Метод Хаффмана (Дерево Хаффмана).
19. Арифметический код.
20. Zip-модификация алгоритма Лемпеля-Зива.
21. LZW-модификация алгоритма Лемпеля-Зива.
22. Профилактика заражения вирусами. Поиск и удаление шпионских и рекламных модулей
23. Криптографические методы защиты.
24. Протоколы аутентификации. Слабости парольных протоколов аутентификации. Виды атак и угроз для протоколов аутентификации.
25. Протоколы электронной подписи. Общие понятия и определения. Виды атак и угроз для протоколов электронной подписи
26. Электронная цифровая подпись.
27. Архитектура системы безопасности ОС.
28. Управление информационной безопасности.

Критерии и шкала оценивания по оценочному средству «устный опрос»

Шкала оценивания (интервал баллов)	Критерий оценивания
5	Ответ представлен на высоком уровне (студент в полном объеме осветил рассматриваемую проблематику, привел аргументы в пользу своих суждений, владеет профильным понятийным (категориальным) аппаратом и т.п.)
4	Ответ представлен на среднем уровне (студент в целом осветил рассматриваемую проблематику, привел аргументы в пользу своих суждений, допустив некоторые неточности и т.п.)
3	Ответ представлен на низком уровне (студент допустил существенные неточности, изложил материал с ошибками, не владеет в достаточной степени профильным категориальным аппаратом и т.п.)
2	Ответ представлен на неудовлетворительном уровне или не представлен (студент не готов, не выполнил задание и т.п.)

Контрольная работа (по вариантам)

Контрольная работа включает выполнение заданий по вариантам и содержит тематические разделы согласно перечню практических работ рабочей программы дисциплины. Решения типовых примеров приводится в методических указаниях к практическим занятиям по дисциплине.

Вариант индивидуального заданий контрольной работы по теме: "ОБРАТИМОЕ XOR ШИФРОВАНИЕ ТЕКСТА СО СЛУЧАЙНОЙ ГАММОЙ"

Получить исходное сообщение, которое было зашифровано при помощи обратимого XOR шифрования.

Гамма = 1234567890123456789

1. Закодированное сообщение: щЯЗЪЕЪЧОСП
2. Закодированное сообщение: еБЮЮГЮЩХСАЯРУЩЭУ
3. Закодированное сообщение: цТКЬЗЦЬЩЭЬЙЖ
4. Закодированное сообщение: рЧФЪЪЦЖХЧБГО
5. Закодированное сообщение: ьТЧСУЫЩЙЛМ
6. Закодированное сообщение: мШЭЩЫЪЯТЩ
7. Закодированное сообщение: ыЪТСЕЫТКСЪС
8. Закодированное сообщение: аЪВЖРЪЧЮРИЪБП
9. Закодированное сообщение: юВЭЧЕЦЫФЩ
10. Закодированное сообщение: юВЭВРЗЖХВЩ
11. Закодированное сообщение: щЯЗЪЕЪЧКСЪС
12. Закодированное сообщение: вЭГФЧЭТХСХ
13. Закодированное сообщение: юВЭЧШШРРЙЮУТЮЬР
14. Закодированное сообщение: аЪЮЖРСЯИЧТСАП
15. Закодированное сообщение: ыЬЮЖЕШЬДФЯГБЗЪЦ

16. Закодированное сообщение: сЩРЪЕЮЕФ
17. Закодированное сообщение: юЧГСЩУЪХЩП
18. Закодированное сообщение: гЧЖЩЫЭЩЫСШ
19. Закодированное сообщение: ыЬЯЫЙИЕЭЙ
20. Закодированное сообщение: сЯУЯЭСЯИЧТСАП

Критерии и шкала оценивания по оценочному средству «задания (по вариантам)»

Шкала оценивания (интервал баллов)	Критерий оценивания
5	Задание выполнено на высоком уровне (правильные ответы даны на 90-100% вопросов/задач)
4	Задание выполнено на среднем уровне (правильные ответы даны на 75-89% вопросов/задач)
3	Задание выполнено на низком уровне (правильные ответы даны на 50-74% вопросов/задач)
2	Задание выполнено на неудовлетворительном уровне (правильные ответы даны менее чем на 50%)

Тесты

Компетенция ОПК-6: Способен использовать современные информационные технологии и программные средства при решении профессиональных задач

Задания закрытого типа

1. Состояние защищенности национальных интересов страны в информационной сфере от внутренних и внешних угроз это:
   a) **Информационная безопасность**
   b) Безопасность
   c) Национальная безопасность
   d) Защита информации

2. Вся накопленная информация об окружающей нас действительности, зафиксированная на материальных носителях или в любой другой форме, обеспечивающая ее передачу во времени и пространстве между различными потребителями для решения научных, производственных, управленческих и других задач
   a) **Информационные ресурсы**
   b) Информационная система
   c) Информационная сфера
   d) Информационные услуги
   e) Информационные продукты

3. Информация не являющаяся общедоступной, которая ставит лиц, обладающих ею в силу своего служебного положения в преимущественное положение по сравнению с другими объектами.

a) служебная информация
b) коммерческая тайна
c) банковская тайна
d) конфиденциальная информация

4. Создание и использование средств опасного воздействия на информационные сферы других стран мира и нарушение нормального функционирования информационных и телекоммуникационных систем это….
   a) **информационная война**
   b) информационное оружие
   c) информационное превосходство

5. Информационно упорядоченная совокупность документов и информационных технологий, реализующая информационные процессы
   a) Информационные ресурсы
   b) **Информационная система**
   c) Информационная сфера
   d) Информационные услуги
   e) Информационные продукты

6. Аппаратно-программные средства криптографической защиты информации выполняют функции:
   a) аутентификацию пользователя, разграничение доступа к информации, обеспечение целостности информации и ее защиты от уничтожения, шифрование и электронную цифровую подпись;
   b) организовывают реализацию политики безопасности информации на этапе эксплуатации КС;
   c) проверяют на отсутствие закладок приборов, устройств.

7. Возможные каналы утечки информации по классификации разделяют:
   a) человек, линия связи;
   b) коммутационное оборудование, человек.
   c) человек, аппаратура, программа;

8. Асимметричная криптосистема предполагает использование
   a) системы разграничения доступа;
   b) двух ключей открытого и личного (секретного);
   c) переносных носителей для хранения секретной информации.

9. Под компьютерным вирусом понимается:
   a) программа имеющая доступ к файлам системы, и имеющая возможность работать с процессами системы;
   b) автономно функционирующая программа, обладающая способностью к самостоятельному внедрению в тела других программ и последующему самовоспроизведению и самораспространению в информационно-вычислительных сетях и отдельных ЭВМ;
   c) программа не имеющая доступ к файлам системы, и не имеющая возможность работать с процессами системы.

10. Надежность защиты информации в компьютерной системе определяется:
    a) конкретным перечнем и свойствами функций КС;
    b) используемыми в функциях КС методами;

c) варианты a) и b)

11. К группе каналов утечки информации, в которой основным средством является человек, относятся следующие утечки:
    a) расшифровка программой зашифрованной информации;
    b) несанкционированный доступ программы к информации;
    c) копирование программой информации с носителей.

12. Атакой на КС называют:
    a) возможность возникновения на каком-либо этапе жизненного цикла КС такого ее состояния, при котором создаются условия для реализации угроз безопасности информации;
    b) событие или действие, которое может вызвать изменение функционирования КС, связанное с нарушением защищенности обрабатываемой в ней информации;
    c) действие, предпринимаемое нарушителем, которое заключается в поиске и использовании той или иной уязвимости.

13. Авторизация– это:
    a) предоставлением полномочий;
    b) подтверждение подлинности;
    c) цифровая подпись.

14. Мандатный метод основывается на:
    a) многоуровневой модели защиты;
    b) использование матриц доступа;
    c) криптографическом преобразовании.

15. Использование аппаратных средств снимает проблему:
    a) обеспечения целостности системы;
    b) разграничение прав пользователей и обслуживающего персонала по доступу к ресурсам КС в соответствии с функциональными обязанностями должностных лиц;
    c) использования строго определенного множества программ.

16. К группе каналов утечки информации, в которой основным средством является аппаратура, относятся следующие утечки:
    a) хищение носителей информации (магнитных дисков, дискет, лент) ;
    b) копирование программой информации с носителей
    c) подключение к ПЭВМ специально разработанных аппаратных средств, обеспечивающих доступ к информации;

17. К группе каналов утечки информации в которой основным средством является программа, относятся следующие утечки:
    a) несанкционированный доступ программы к информации;
    b) хищение носителей информации(магнитных дисков, дискет, лент);
    c) использование специальных технических средств для перехвата электромагнитных излучений технических средств ПЭВМ.

18. Какая из функций не входит в процесс управления ключами?
    a) генерация ключей;
    b) распределение ключей.
    c) переадресация ключей;

19. Резидентные вирусы это:

a) вирусы, которые выполняются только в момент запуска зараженной программы;

b) вирусы, которые после активизации постоянно находятся в оперативной памяти компьютера и контролируют доступ к его ресурсам;

c) вирусы, заражающие программы, хранящиеся в системных областях дисков.

20. К непреднамеренным угрозам относятся:

a) ошибки в разработке программных средств КС;

b) несанкционированный доступ к ресурсам КС со стороны пользователей КС и посторонних лиц, ущерб от которого определяется полученными нарушителем полномочиями;

c) угроза нарушения конфиденциальности, т.е. утечки информации ограниченного доступа, хранящейся в КС или передаваемой от одной КС к другой.

21. Для проведения процедур идентификации и аутентификации пользователя необходимо:

a) наличие соответствующего субъекта (модуля) аутентификации;

b) наличие аутентифицирующего объекта, хранящего уникальную информацию;

c) ответы a) и b)

22. Какой из функциональных блоков должна содержать система разграничения доступа к информации:

a) блок криптографического преобразования информации при ее хранении и передаче;

b) блок контроля среды размещения;

c) блок контроля среды выполнения.

23. К средствам активной защиты относятся:

a) искаженные программы (программы вирусы, искажение функций) ;

b) заказное проектирование;

c) специальная аппаратура.

24. К умышленным угрозам относятся:

a) воздействие на аппаратные средства КС физических полей других электронных устройств(при несоблюдении условий их электромагнитной совместимости) и др.

b) ошибки пользователей КС.

c) несанкционированные действия обслуживающего персонала КС (например, ослабление политики безопасности администратором, отвечающим за безопасность КС);

25. Биометрическая идентификация и аутентификация пользователя это:

a) схема идентификации позволяющая увеличить число аккредитаций, выполняемых за один цикл, и тем самым уменьшить длительность процесса идентификации;

b) идентификация потенциального пользователя путем измерения физиологических параметров и характеристик человека, особенностей его поведения;

c) схема идентификации с нулевой передачей знаний.

26. Косвенными каналами утечки называют:

a) каналы, не связанные с физическим доступом к элементам КС;

b) каналы, связанные с физическим доступом к элементам КС;

c) каналы, связанные с изменение элементов КС и ее структуры.

27. Для чего используется процедура “рукопожатия”:
a) для распределения ключей между подлинными партнерами;
b) для взаимной проверки подлинности;
c) для безопасного использования интеллектуальных карт.

28. Модификация ключа– это
a) генерирование нового ключа из предыдущего значения ключа с помощью односторонней (однонаправленной) функции;
b) генерирование нового ключа из последующего значения ключа с помощью односторонней(однонаправленной) функции;
c) генерирование нового ключа из предыдущего значения ключа с помощью двусторонней(двунаправленной) функции.

29. Транзитные вирусы это:
a) вирусы, которые после активизации постоянно находятся в оперативной памяти компьютера и контролируют доступ к его ресурсам;
b) вирусы, которые выполняются только в момент запуска зараженной программы;
c) вирусы, заражающие программы, хранящиеся в системных областях дисков.

30. Под организацией доступа к ресурсам понимается
a) хранения атрибутов системы защиты, поддержки криптографического закрытия информации, обработки сбоев и отказов и некоторые другие;
b) предотвращение несанкционированного перехода пользовательских процессов в привилегированное состояние.
c) весь комплекс мер, который выполняется в процессе эксплуатации КС для предотвращения несанкционированного воздействия на технические и программные средства, а также на информацию;

31. Технические мероприятия направлены:
a) на использование специальных технических средств для перехвата электромагнитных излучений технических средств ПЭВМ;
b) на защиту ключей шифрования и электронной цифровой подписи(ЭЦП) и неизменность алгоритма шифрования и ЭЦП.
c) на недопущение выхода информативного сигнала за пределы контролируемой территории с помощью сертифицированных технических средств защиты;

32. Вирусы-мутанты (MtE-вирусы) это
a) вирусы, содержащие в себе алгоритмы шифрования, обеспечивающие различие разных копий вируса;
b) вирусы, пытающиеся быть невидимыми на основе контроля доступа к зараженным элементам данных;
c) вирусы, заражающие программы, хранящиеся в системных областях дисков.

33. Каким из перечисленных способов не реализуется распределение ключей между пользователями компьютерной сети:
a) документирование алгоритмов обеспечения защиты информации;
b) использованием одного или нескольких центров распределения ключей;
c) прямым обменом сеансовыми ключами между пользователями сети.

34. Активные способы защиты информации при ее утечке через сеть электропитания направленные на:
    а) создание маскирующего шума;
    b) перехвата информации;
    c) минимизацию паразитных связей внутри ПЭВМ.

35. Механизм запроса-ответа используется для:
    а) проверки подлинности;
    b) шифрования;
    c) регистрации времени для каждого сообщения.

Задания открытого типа

1. Продолжите фразу: " Последовательность символов, недоступная для посторонних, предназначенная для идентификации и аутентификации субъектов и объектов между собой - это..."_____(**пароль**)

2. Информация может быть защищена без аппаратных и программных средств защиты с помощью _____преобразований. Запишите ответ: _____ (**криптографических/криптографии**)

3. Символы шифруемого текста последовательно складываются с символами некоторой специальной последовательности, это метод _____ (**гаммирования/гаммирование**)

4. Получить исходное сообщение, которое было зашифровано.

Для шифрования сообщения был применен комбинированный подход:
1) Перестановка (по методу Гамильтона), 5-2-1-6-4-8-7-3;
2) Обратимое XOR шифрование, 1234567890123456789
Закодированное сообщение: УЭаЯХЫТИдХЩпойил
Слово: Управление

5. Получить исходное сообщение, которое было зашифровано.

Для шифрования сообщения был применен комбинированный подход:
1) Перестановка (по методу Гамильтона), 5-2-1-6-4-8-7-3;
2) Обратимое XOR шифрование, 1234567890123456789
Закодированное сообщение: ЯШоШШБЯЦРБФпЫйиЬ
Слово: Экономический

6. Получить исходное сообщение, которое было зашифровано.

Для шифрования сообщения был применен комбинированный подход:
1) Перестановка (по методу Гамильтона), 5-2-1-6-4-8-7-3;
2) Обратимое XOR шифрование, 1234567890123456789
Закодированное сообщение: БЯыШЫАЧМдПЩпойил
Слово: Информация

7. Получить исходное сообщение, которое было зашифровано.

Для шифрования сообщения был применен комбинированный подход:
1) Перестановка (по методу Гамильтона), 5-2-1-6-4-8-7-3;
2) Обратимое XOR шифрование, 1234567890123456789
Закодированное сообщение: ГТфФЭЮжБдВАпЯйиУ

Слово: ЗащитаСистем

8. Получить исходное сообщение, которое было зашифровано.
Для шифрования сообщения был применен комбинированный подход:
1) Перестановка (по методу Гамильтона), 5-2-1-6-4-8-7-3;
2) Обратимое XOR шифрование, 1234567890123456789
Закодированное сообщение: ЧТюЩРЗЩЬдМГпойил
Слово: Надежность

9. Получить исходное сообщение, которое было зашифровано.
Для шифрования сообщения был применен комбинированный подход:
1) Перестановка (по методу Гамильтона), 5-2-1-6-4-8-7-3;
2) Обратимое XOR шифрование, 1234567890123456789
Закодированное сообщение: ЯЪлЦЕЫЧМдХЩпойил
Слово: Шифрование

10. Получить исходное сообщение, которое было зашифровано.
Для шифрования сообщения был применен комбинированный подход:
1) Перестановка (по методу Гамильтона), 5-2-1-6-4-8-7-3;
2) Обратимое XOR шифрование, 1234567890123456789
Закодированное сообщение: ГЦыЬШЮГЭЖРЫпЫйиА
Слово: Идентификация

11. Получить исходное сообщение, которое было зашифровано.
Для шифрования сообщения был применен комбинированный подход:
1) Перестановка (по методу Гамильтона), 5-2-1-6-4-8-7-3;
2) Обратимое XOR шифрование, 1234567890123456789
Закодированное сообщение: ЬБуЖРВЯКСЪЩНЕйиЦ
Слово: Аутентификация

12. Получить исходное сообщение, которое было зашифровано.
Для шифрования сообщения был применен комбинированный подход:
1) Перестановка (по методу Гамильтона), 5-2-1-6-4-8-7-3;
2) Обратимое XOR шифрование, 1234567890123456789
Закодированное сообщение: ЬЬшыЭЖЧЫдЫЯпойиК
Слово: ЛогинПароль

13. Получить исходное сообщение, которое было зашифровано.
Для шифрования сообщения был применен комбинированный подход:
1) Перестановка (по методу Гамильтона), 5-2-1-6-4-8-7-3;
2) Обратимое XOR шифрование, 1234567890123456789
Закодированное сообщение: ГЩоДЯЫЩЭТЛЬМщйВЯ
Слово: ЭлектронныйКлюч

14. Получить исходное сообщение, которое было зашифровано.
Для шифрования сообщения был применен комбинированный подход:
1) Перестановка (по методу Гамильтона), 5-2-1-6-4-8-7-3;
2) Обратимое XOR шифрование, 1234567890123456789
Закодированное сообщение: ЩЧвАЗЬЯИдВСпойил
Слово: Сертификат

15. Получить исходное сообщение, которое было зашифровано.
Для шифрования сообщения был применен комбинированный подход:
1) Перестановка (по методу Гамильтона), 5-2-1-6-4-8-7-3;
2) Обратимое XOR шифрование, 1234567890123456789

Закодированное сообщение: ЩЩтДЯФЩЦдШИпойиЬ
Слово: Блокировщик

16. Получить исходное сообщение, которое было зашифровано.
Для шифрования сообщения был применен комбинированный подход:
1) Перестановка (по методу Гамильтона), 5-2-1-6-4-8-7-3;
2) Обратимое XOR шифрование, 1234567890123456789
Закодированное сообщение: ГТфФЭЦгБдЫШпСйиШ
Слово: ЗащитаФайлов

17. Получить исходное сообщение, которое было зашифровано.
Для шифрования сообщения был применен комбинированный подход:
1) Перестановка (по методу Гамильтона), 5-2-1-6-4-8-7-3;
2) Обратимое XOR шифрование, 1234567890123456789
Закодированное сообщение: БЭуФХЫЕЧдЩКпойил
Слово: Аппаратный

18. Поддельные сообщения от имени банков или финансовых компаний, целью которых является сбор логинов, паролей и пин-кодов пользователей называется _____(**фишинг**)
19. Одиночная **атаки**, в котором мошенники нападают с целью вызвать перегрузку подсистемы сервиса, путём отправки максимального количества трафика жертве. _____(**DoS-атака**)
20. На каком уровне эталонной семиуровневой модели может быть реализовано туннелирование? _____(**сетовом/сетевом уровне**)
21. Профессиональные взломщики защиты компьютерных программ и создатели компьютерных вирусов _____(**хакеры**)
22. Процесс входа в систему, который состоит из нескольких шагов и требует от пользователя указать больше информации, а не только пароль _____(**многоступенчатая аутентификация/ MFA**)
23. Запирающее устройство, которое работает с помощью электрического тока _____(**электронный замок**)
24. Протокол, который обеспечивает целостность и конфиденциальность данных при их передаче между сайтом и устройством пользователя _____ (**https / HyperText Transfer Protocol Secure**)
25. Технология виртуализации данных, которая объединяет несколько дисков в логический элемент для избыточности и повышения производительности _____ (**RAID / RAID-массив/ избыточный массив независимых дисков**)
26. Основная составляющая информационной безопасности, обеспечивающая защиту важной информации от несанкционированного доступа к информации называется _____(**конфиденциальность**)
27. Основная составляющая информационной безопасности, обеспечивающая возможность работы с информацией и за приемлемое время получить требуемую информационную услугу называется _____(**доступность**)
28. Основная составляющая информационной безопасности, обеспечивающая неизменности данных при выполнении какой-либо операции над ними называется _____(**целостность**)
29. Если вы покидаете рабочее место менее чем на 10 минут, какой комбинацией клавиш можно блокировать компьютер в ОС Windows? _____(**Win+L**)
30. Вид вредоносных программ, способных внедряться в код других программ, системные области памяти, загрузочные секторы и распространять свои копии по

разнообразным каналам связи _____ (**компьютерные вирусы / вирусы**)

На сопоставление или ранжирование

1. Установите соответствие:

1) преднамеренные угрозы	а) хищение информации
2) случайные угрозы	б) ошибки пользователя
	в) компьютерные вирусы
	г) отказы и сбои аппаратуры
	д) физическое воздействие на аппаратуру
	е) форс-мажорные обстоятельства

Ответ: 1-а,в,д 2-б,г,е,

2. Установите соответствие:

1) Антивирус обеспечивает поиск вирусов в оперативной памяти, на внешних носителях путем подсчета и сравнения с эталоном контрольной суммы	а) доктор
2) Антивирус представляет собой небольшую резидентную программу, предназначенную для обнаружения подозрительных действий при работе компьютера, характерных для вирусов	б) сторож
3) Антивирус запоминает исходное состояние программ, каталогов и системных областей диска когда компьютер не заражен вирусом, а затем периодически или по команде пользователя сравнивает текущее состояние с исходным	в) ревизор
4) Антивирус не только находит зараженные вирусами файлы, но и "лечит" их, т.е. удаляет из файла тело программы вируса, возвращая файлы в исходное состояние	г) детектор

Ответ: 1-г; 2-б; 3-в; 4-а

3. Разместите виды информационной безопасности от верхнего к нижнему уровню
Корпоративная
Персональная
Государственная

1) государственная
2) корпоративная,
3) персональная,

4. Установите соответствие:

1) кодирование
2) рассечение-разнесение
3) сжатие-расширение

а) переход от одной формы представления информации к другой, более удобной для хранения, передачи или обработки
б) замену часто встречающихся одинаковых последовательностей символов некоторыми заранее выбранными символами или же подмешивание дополнительной информации
в) массив защищенных. данных делится на части, каждая из которых в отдельности не позволяет раскрыть содержание защищаемой информации

Ответ: 1а 2в 3б

5. Установите соответствие:

1. стандарт ISO/IEC 27000
2. CobiT
3. ITIL

а) принципы управления и аудита информационных технологий
б) система менеджмента информационной безопасности
в) руководств по управлению, отладке и постоянного улучшения бизнес-процессов, связанных с ИТ

Ответ: 1б 2а 3в

6. Установите соответствие:

1. Разглашение государственной тайны наказывается
2. Разглашение информации, доступ к которой ограничен федеральным законом (за исключением случаев, если разглашение такой информации влечет уголовную ответственность), лицом, получившим доступ к такой информации в связи с исполнением служебных или профессиональных обязанностей влечет
3. Неправомерный доступ к компьютерной информации, если это деяние повлекло уничтожение, блокирование, модификацию либо копирование информации, нарушение работы ЭВМ, системы ЭВМ или их сети, – наказывается
4. Создание, использование и распространение вредоносных программ для ЭВМ, заведомо приводящих к несанкционированному уничтожению, блокированию,

а) штрафом в размере до двухсот тысяч рублей или в размере заработной платы или иного дохода осужденного за период до восемнадцати месяцев, либо исправительными работами на срок до одного года, либо ограничением свободы на срок до двух лет, либо принудительными работами на срок до двух лет, либо лишением свободы на тот же срок
б) арестом на срок от четырех до шести месяцев либо лишением свободы на срок до четырех лет с лишением права занимать определенные должности или заниматься определенной деятельностью на срок до трех лет
в) наложение административного штрафа на гражданина в размере от пятисот до одной тысячи рублей, а на должностного лица – от четырех тысяч до пяти тысяч рублей
г) ограничением свободы на срок до

модификации либо копированию информации, нарушению работы ЭВМ, системы ЭВМ или их сети, а равно ис-пользование либо распространение таких программ или машинных носителей с такими про-граммами – наказываются	четырех лет, либо принудительными работами на срок до четырех лет, либо лишением свободы на тот же срок со штрафом в размере до двухсот тысяч рублей или в размере заработной платы или иного дохода осужденного за период до восемнадцати месяцев.

Ответ: 1б 2в 3а 4г

7. Разместите уровни модели OSI от нижнего у верхнему

Прикладной уровень
Физический уровень
Канальный уровень,
Сеансовый уровень
Сетевой уровень
Транспортный уровень
Представительный уровень

1) Физический уровень
2) Канальный уровень,
3) Сетевой уровень,
4) Транспортный уровень
5) Сеансовый уровень
6) Представительный уровень
7) Прикладной уровень

8. Установите соответствие:

1. Физический уровень	а) доступ к сетевым службам
2. Канальный уровень,	б) представление и кодирование данных
3. Сетевой уровень,	в) управление сеансом связи
4. Транспортный уровень	г) прямая связь между конечными пунктами и надежность
5. Сеансовый уровень	д) определение маршрута и логическая адресация
6. Представительный уровень	е) физическая адресация
7. Прикладной уровень	ж) работа со средой передачи, сигналами и двоичными данными
8.	

Ответ: 1ж 2е 3д 4г 5в 6б 7а

9. Установите соответствие:

1. Конфиденциальность	а) Основная составляющая информационной безопасности, обеспечивающая неизменности данных при выполнении какой-либо операции над ними
2. Доступность	
3. Целостность	б) Основная составляющая информационной безопасности, обеспечивающая защиту важной информации от несанкционированного доступа к информации

в) Основная составляющая информационной безопасности, обеспечивающая возможность работы с информацией и за приемлемое время получить требуемую информационную услугу

Ответ: 1б 2в 3а

10. Установите соответствие:

1. информационно-справочные системы
2. информационно-советующие системы
3. информационно-управляющие системы

а) предназначены для накопления и анализа данных, необходимых для принятия решений в различных сферах деятельности людей
б) вырабатывают информацию, которая принимается человеком к сведению и не превращается немедленно в серию конкретных действий. Эти системы обладают более высокой степенью интеллекта, так как для них характерна обработка знаний, а не данных.
в) компьютерное программное средство, предназначенное для хранения и предъявления пользователю разнообразной информации справочного содержания

Ответ: 1в 2б 3а

Компетенция ОПК-7: Способен понимать принципы работы современных информационных технологий и использовать их для решения задач профессиональной деятельности

Задания закрытого типа

1. Область науки и техники, охватывающая совокупность криптографических, программно-аппаратных, технических, правовых, организационных методов и средств обеспечения безопасности информации при ее обработке, хранении и передаче с использованием современных информационных технологий:
   a) **Комплексное обеспечение информационной безопасности**
   b) Безопасность АС
   c) Угроза безопасности
   d) Атака на автоматизированную систему
   e) Политика безопасности

2. Непрерывный целенаправленный процесс, предполагающий принятие соответствующих мер на всех этапах жизненного цикла АС:
   a) Принцип системности
   b) Принцип комплексности
   c) **Принцип непрерывной защиты**
   d) Принцип разумной достаточности
   e) Принцип гибкости системы

3. Виды информационной безопасности:
   a) Персональная, корпоративная, государственная
   b) Клиентская, серверная, сетевая
   c) Локальная, глобальная, смешанная

4. К основным принципам обеспечения информационной безопасности относится:
   a) Экономической эффективности системы безопасности
   b) Многоплатформенной реализации системы
   c) Усиления защищенности всех звеньев системы

5. Политика безопасности в системе (сети) – это комплекс:
   a) Нормы информационного права, соблюдаемые в сети
   b) Руководств, требований обеспечения необходимого уровня безопасности
   c) Инструкций, алгоритмов поведения пользователя в сети

6. К правовым методам, обеспечивающим информационную безопасность, относятся:
   a) Разработка аппаратных средств обеспечения правовых данных
   b) Разработка и установка во всех компьютерных правовых сетях журналов учета действий
   c) Разработка и конкретизация правовых нормативных актов обеспечения безопасности

7. Документированная информация, доступ к которой ограничивается в соответствии с законодательством РФ:
   a) **Государственная тайна**
   b) Коммерческая тайна
   c) Банковская тайна
   d) Конфиденциальная информация

8. Под угрозой безопасности информации в компьютерной системе (КС) понимают:
   a) возможность возникновения на каком-либо этапе жизненного цикла КС такого ее состояния, при котором создаются условия для реализации угроз безопасности информации;
   b) событие или действие, которое может вызвать изменение функционирования КС, связанное с нарушением защищенности обрабатываемой в ней информации;
   c) действие, предпринимаемое нарушителем, которое заключается в поиске и использовании той или иной уязвимости.

9. Идентификация объекта– это:
   a) одна из функций подсистемы защиты;
   b) взаимное установление подлинности объектов, связывающихся между собой по линиям связи;
   c) сфера действий пользователя и доступные ему ресурсы КС.

10. Уязвимость информации— это:
   a) возможность возникновения на каком-либо этапе жизненного цикла КС такого ее состояния, при котором создаются условия для реализации угроз безопасности информации;
   b) событие или действие, которое может вызвать изменение функционирования КС, связанное с нарушением защищенности обрабатываемой в ней информации;

c) это действие, предпринимаемое нарушителем, которое заключается в поиске и использовании той или иной уязвимости.

11. Что НЕ является элементом системы обеспечения информационной безопасности РФ:
a) Палаты Федерального собрания;
b) Президент;
c) Органы местного самоуправления;
d) **Общественная Палата**;
e) Органы исполнительной власти**;**
f) Совет безопасности?

12. Создание, использование и распространение вредоносных программ для ЭВМ, заведомо приводящих к несанкционированному уничтожению, блокированию, модификации либо копированию информации, нарушению работы ЭВМ, системы ЭВМ или их сети, а равно использование либо распространение таких программ или машинных носителей с такими программами – могут осуществляться
a) только с прямым умыслом
b) по неосторожности

13. Для чего создается система разграничения доступа к информации:
a) для защиты информации от НСД;
b) для осуществления НСДИ;
c) определения максимального уровня конфиденциальности документа.

14. Процедуру установки сфер действия пользователя и доступные ему ресурсы КС называют:
a) аутентификацией;
b) авторизацией;
c) идентификация.

15. Искусственные угрозы исходя из их мотивов разделяются на:
a) косвенные и непосредственные;
b) несанкционированные и санкционированные.
c) непреднамеренные и преднамеренные;

16. Аутентификация – это:
a) подтверждение подлинности;
b) предоставлением полномочий;
c) цифровая подпись.

17. При эксплуатации механизмов аутентификации основными задачами являются:
a) генерация или изготовление идентификаторов, их учет и хранение, передача идентификаторов пользователю и контроль над правильностью выполнения процедур аутентификации в КС;
b) разграничение прав пользователей и обслуживающего персонала по доступу к ресурсам КС в соответствии с функциональными обязанностями должностных лиц;
c) реализация механизма виртуальной памяти с разделением адресных пространств.

18. Организационными мероприятиями предусматривается
a) исключение нахождения в местах наличия информативного сигнала злоумышленника и контроль за его действиями и передвижением;

b) исключение значительной части загрузочных модулей из сферы их досягаемости;
c) исключение несанкционированного доступа к ресурсам ПЭВМ и хранящимся в ней программам и данным.

19. Избирательная политика безопасности подразумевает, что:
a) права доступа субъекта к объекту системы определяются на основании некоторого внешнего (по отношению к системе) правила (свойство избирательности);
b) все субъекты и объекты системы должны быть однозначно идентифицированы;
c) каждому объекту системы присвоена метка критичности, определяющая ценность содержащейся в нем информации.

20. В чем заключается правило разграничения доступа
a) лицо допускается к работе с документом только в том случае, если уровень допуска субъекта доступа равен или выше уровня конфиденциальности документа, а в наборе категорий, присвоенных данному субъекту доступа, содержатся все категории, определенные для данного документа;
b) лицо допускается к работе с документом только в том случае, если уровень допуска субъекта доступа ниже уровня конфиденциальности документа, а в наборе категорий, присвоенных данному субъекту доступа, содержатся все категории, определенные для данного документа;
c) лицо допускается к работе с документом только в том случае, если уровень допуска субъекта доступа ниже уровня конфиденциальности документа, а в наборе категорий, присвоенных данному субъекту доступа, не содержатся все категории, определенные для данного документа.

21. Полномочная политика безопасности подразумевает, что:
a) каждому субъекту системы присвоен уровень прозрачности (security clearance), определяющий максимальное значение метки критичности объектов, к которым субъект имеет доступ;
b) все субъекты и объекты системы должны быть идентифицированы;
c) права доступа субъекта к объекту системы определяются на основании некоторого внешнего(по отношению к системе) правила (свойство избирательности).

22. Уязвимость информации— это:
a) неизменность информации в условиях ее случайного и(или) преднамеренного искажения или разрушения.
b) возможность возникновения на каком-либо этапе жизненного цикла КС такого ее состояния, при котором создаются условия для реализации угроз безопасности информации;
c) набор документированных норм, правил и практических приемов, регулирующих управление, защиту и распределение информации ограниченного доступа;

23. Достоверная вычислительная база- это:
a) активный компонент системы, который может явиться причиной потока информации от объекта к объекту или изменения состояния системы;

b) абстрактное понятие, обозначающее полностью защищенный механизм вычислительной системы (включая аппаратные и программные средства), отвечающий за поддержку реализации политики безопасности;
c) пассивный компонент системы, хранящий, принимающий или передающий информацию.

24. Какой метод может противодействовать дизассемблированию
a) шифрование;
b) хэширование;
c) изучение.

25. Методы, затрудняющие считывание скопированной информации основываются на
a) придании особенностей процессу записи информации, которые не позволяют считывать полученную копию на других накопителях, не входящих в защищаемую КС;
b) разграничении прав пользователей и обслуживающего персонала по доступу к ресурсам КС в соответствии с функциональными обязанностями должностных лиц;
c) использования дополнительных программных или аппаратно-программных средств.

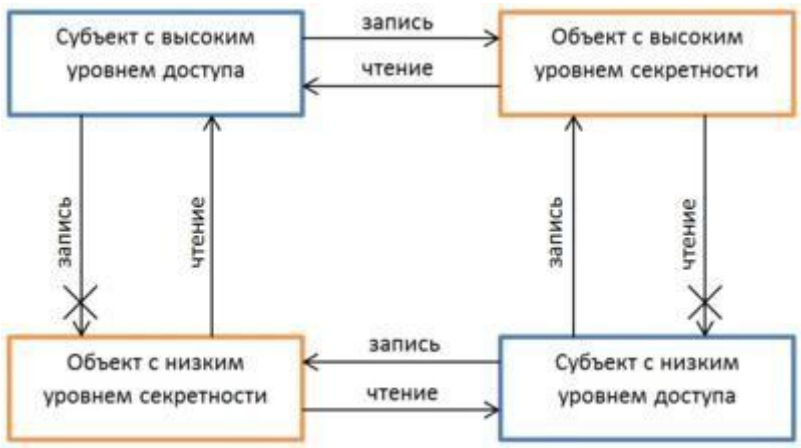
26. Троянские программы это:
a) программы, содержащие в себе алгоритмы шифрования, обеспечивающие различие разных копий вируса;
b) программы которые содержат скрытые последовательности команд (модули), выполняющие действия, наносящие вред пользователям;
c) программы которые после активизации постоянно находятся в оперативной памяти компьютера и контролируют доступ к его ресурсам.

27. Укажите пароль, который отвечает требованиям сложности пароля и не является слабым.
a) YaStudent100%
b) Password_111
c) 84c3M#@kH$&1
d) #1XE@
e) Qwer_1234567890

28. Укажите возможные методы восстановления пароля в программах вкрытия паролей
a) Перебор по маске
b) Атака по словарю
c) Прямой перебор
d) По электронной почте

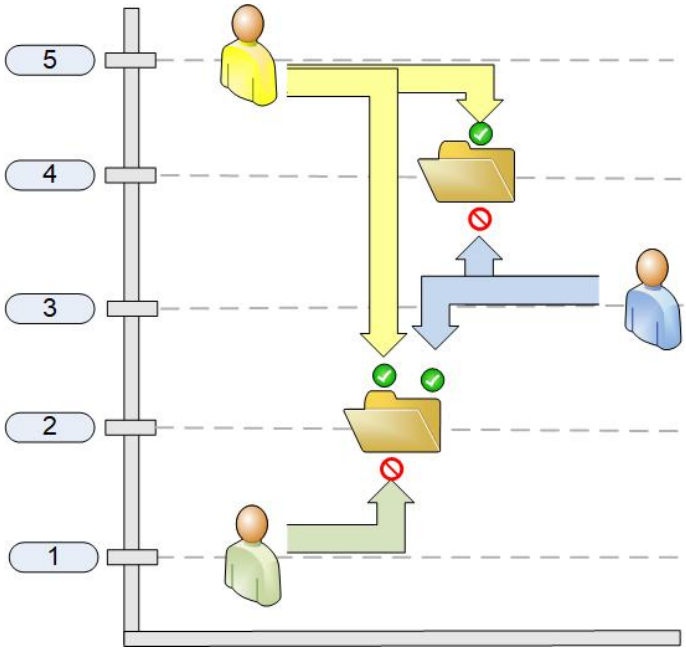
29. Для чего служат сети VPN (укажите правильный ответ)?
a) для обеспечения соединения трёх видов: узел-узел, узел-сеть и сеть-сеть (в зависимости от применяемых протоколов)
b) для обеспечения сетевых соединений поверх другой сети (например, Интернет)
c) для улучшения безопасности локальной сети
d) для увеличения быстродействия локальной сети

30. Как называется модель разграничения доступа к защищаемой информации, приведенная на рисунке.



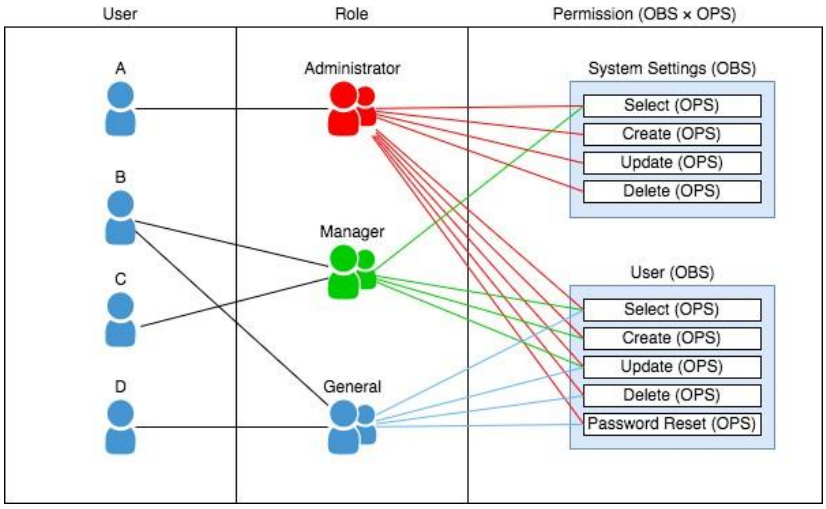
a) **Модель Белла-Лападулы**
b) Модель Фостера-Стюарта
c) Модель Бокса-Дженкинса

31. Схема какой модели управления доступом представлена на рисунке?



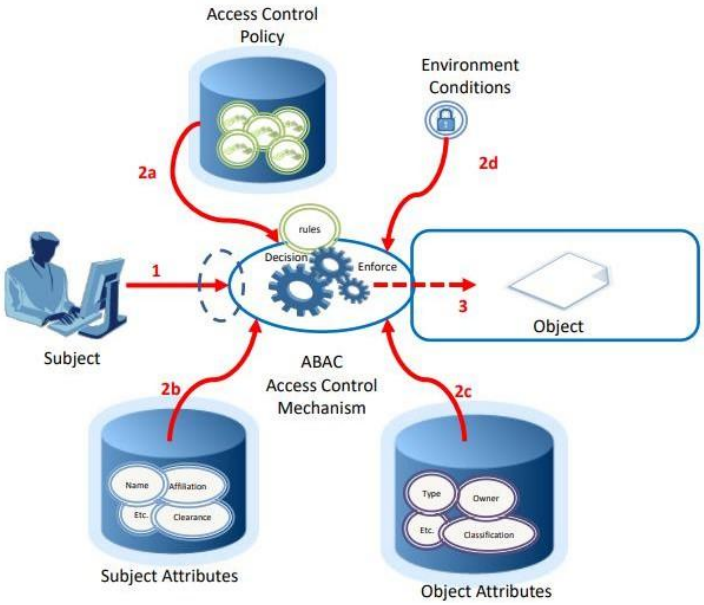
a) дискреционная модель управления;
b) мандатная модель управления;
c) ролевая модель управления;
d) управление доступом на основе правил

32. Схема какой модели управления доступом представлена на рисунке?



a) дискреционная модель управления;
b) мандатная модель управления;
c) ролевая модель управления;
d) управление доступом на основе правил

33. Схема какой модели управления доступом представлена на рисунке?



a) дискреционная модель управления;
b) мандатная модель управления;
c) ролевая модель управления;
d) управление доступом на основе правил

34. Схема какой модели управления доступом представлена на рисунке?
a) дискреционная модель управления;
b) мандатная модель управления;
c) ролевая модель управления;
d) управление доступом на основе правил

35. Какие права предоставлены к объекту группе "хозяина" -rw-r--r--
   a) только чтение
   b) только запись
   c) чтение и запись

36. Какие права предоставлены к объекту группе "все остальные" -rw-r--r--
   a) только чтение
   b) только запись
   c) чтение и запись

37. Какой метод создания резервных копий представлен на рисунке?

   a) **Полное резервное копирование**
   b) Инкрементное резервное копирование
   c) Дифференциальное резервное копирование

38. Какой метод создания резервных копий представлен на рисунке?

   a) Полное резервное копирование
   b) Инкрементное резервное копирование
   c) Дифференциальное резервное копирование

39. Какой метод создания резервных копий представлен на рисунке?

a) Полное резервное копирование
b) Инкрементное резервное копирование
c) Дифференциальное резервное копирование

40. Наиболее важным при реализации защитных мер политики безопасности является:
a) Аудит, анализ затрат на проведение защитных мер
b) Аудит, анализ уязвимостей, риск-ситуаций
c) Аудит, анализ безопасности

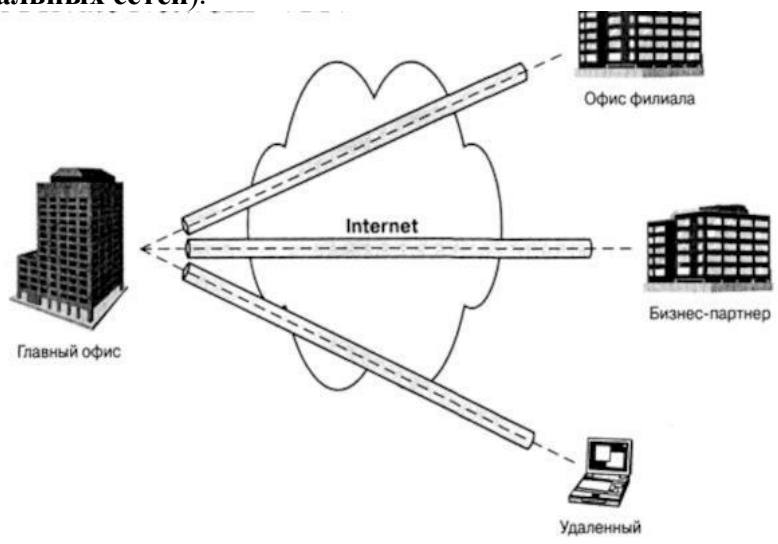
Задания открытого типа

1. Состояние защищенности жизненно важных интересов личности, общества, государства в информационной сфере (среде)_____ (**информационная безопасность**)

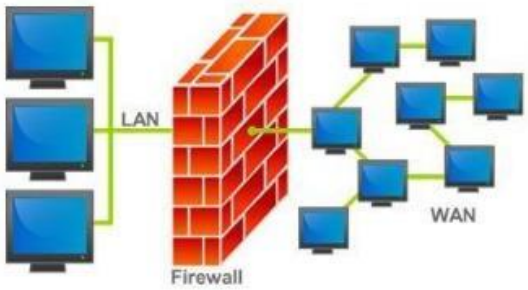
2. Максимальный срок лишения свободы за незаконное получение и разглашение сведений, составляющих коммерческую тайну (лет) _____**(5 лет/5)**

3. Метод специального преобразования информации, с целью защиты от ознакомления и модификации посторонним лицом _____(**криптография**)

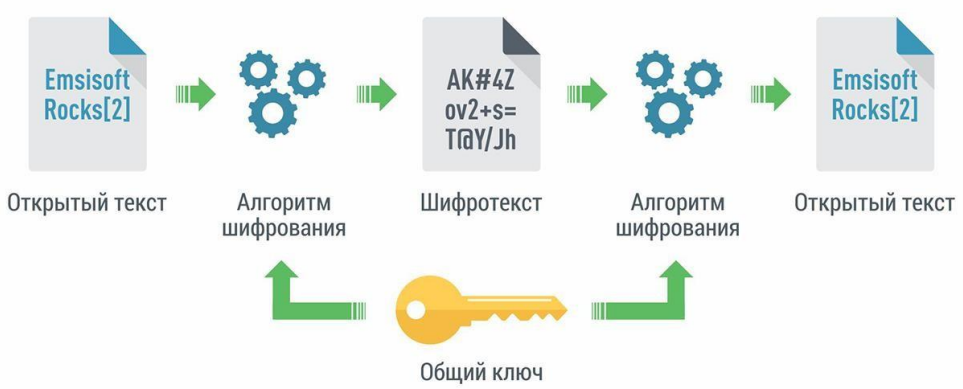
4. Какая технология построения сетей изображена на рисунке ниже. _____ (**VPN/виртуальных сетей**).



5. Какой комплекс программно-аппаратных средств, осуществляющий информационную защиту одной части компьютерной сети от другой путем анализа, проходящего между ними трафика изображен на рисунке? _____(**файервол /брандмауэр/межсетевой экран**)

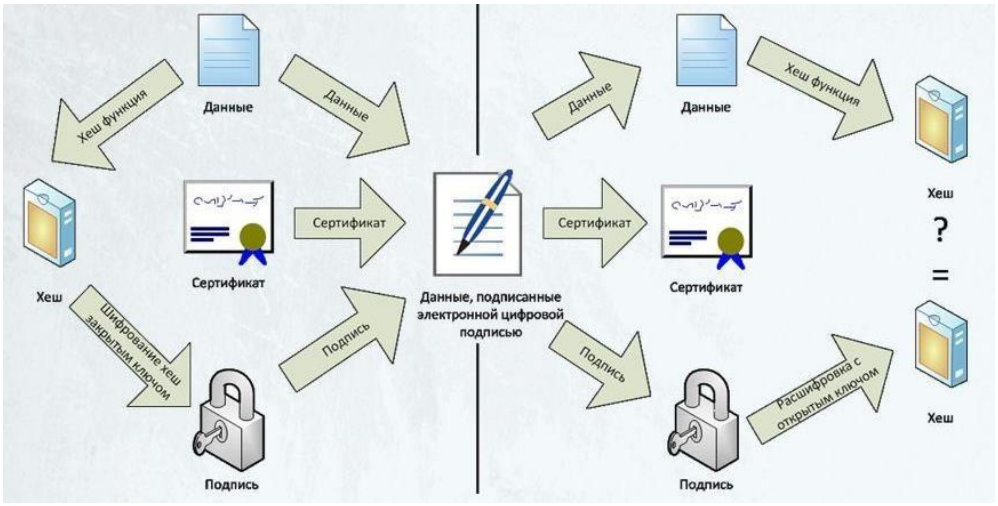


6. Схема какого метода закрытия информации представлена на рисунке? _____(**Симметричное шифрование/симметричного**)



7. Схема какого метода закрытия информации представлена на рисунке? _____(**асимметричное шифрование/ассиметричного**)

8. Схема какого метода закрытия информации представлена на рисунке? _____(**электронная цифровая подпись/ЭЦП**)



9. Как называется способ передачи или хранения информации путем сокрытия самого факта такой передачи/хранения, результат, которого представлен на рисунке? _____(**Стеганография**)

10. Представление информации в виде условных сигналов с целью автоматизации ее хранения, обработки, передачи и т.д. _____(**кодирование**).
11. Продолжите фразу: "Административная и законодательная мера, соответствующая мере ответственности лица за потерю конкретной секретной информации, регламентирующаяся специальным документом с учетом государственных и военно-стратегических, коммерческих или частных интересов - это..." Запишите ответ: _____ (**уровень секретности**)
12. Потенциально возможное событие, действие, процесс или явление, которое может причинить ущерб чьих-нибудь данных, называется _____(**угроза**)
13. Доступ к информации в нарушение должностных полномочий сотрудника, доступ к закрытой для публичного доступа информации со стороны лиц, не имеющих разрешения на доступ к этой информации называется _____ (**несанкционированным доступом**)
14. Метод пароля и его модификация, метод вопрос-ответ, метод секретного алгоритма - это методы _____(**аутентификации**)
15. Совокупность документированных правил, процедур, практических приемов или руководящих принципов в области безопасности информации, которыми

руководствуется организация в своей деятельности называется _____(**политикой безопасности**)

16. Лицо, пытающееся посредством использования несовершенства правовых, организационных или технических средств обеспечения информационной безопасности оказать неправомерное и несанкционированное воздействие на (получить, изменить или ограничить в доступе защищаемую информацию) информацию организации _____(**злоумышленник**)
17. Действие некоторого субъекта компьютерной системы (пользователя, программы, процесса и т.д.), использующего уязвимость компьютерной системы для достижения целей, выходящих за пределы авторизации данного субъекта в компьютерной системе. _____(**атака**)
18. Состояние защищенности жизненно важных интересов личности, общества и государства от внутренних и внешних угроз — это _____(**безопасность**)
19. Сведения о фактах, событиях и обстоятельствах жизни гражданина, позволяющие идентифицировать его личность _____(**персональные данные)**
20. Система штатных органов управления и организационных формирований, предназначенных для обеспечения безопасности информации предприятия _____(**служба безопасности**)
21. Сколько текстовой информации может быть скрыто методами стеганографии в цветной фотографии, сделанной 3-х мегапиксельной камерой мобильного телефона?
22. Сколько текстовой информации может быть скрыто методами стеганографии в цветной фотографии формата bmp, сделанной мегапиксельной камерой мобильного телефона?
23. Сколько текстовой информации может быть скрыто методами стеганографии в 30 секундах моно-звучания на ПК музыкального фрагмента в формате wav?
24. Сколько текстовой информации может быть скрыто методами стеганографии в 30 секундах стерео-звучания на ПК музыкального фрагмента в формате wav?
25. Сколько текстовой информации может быть скрыто методами стеганографии в 1 странице текстового файла на русском языке?
26. Сколько текстовой информации может быть скрыто методами стеганографии в 1 странице текстового файла на английском языке?
27. Сколько текстовой информации может быть скрыто методами стеганографии в 100-минутном фильме, записанном на DVD-диск в стандарте SECAM?
28. Сколько текстовой информации может быть скрыто методами стеганографии в 100-минутном фильме, записанном на DVD-диск в стандарте NTSC?
29. Работник обязан не разглашать коммерческую тайну после прекращения трудового договора в течение _____ лет или срока, предусмотренного соглашением между сотрудником и работодателем, заключенным в период срока действия трудового договора. (**3 лет**)
30. Неправомерный доступ к компьютерной информации, если это деяние повлекло уничто-жение, блокирование, модификацию либо копирование информации, нарушение работы ЭВМ, системы ЭВМ или их сети, – наказывается _____ (**штрафом**)

На сопоставление или ранжирование

1. Расположите уровни обеспечения информационной безопасности в РФ от высшего к низшему: **1**) программно-аппаратный; **2**) административный (организационный); **3**) законодательно-правовой;

Ответ:
1) законодательно-правовой;
2) административный (организационный);

3) программно-аппаратный

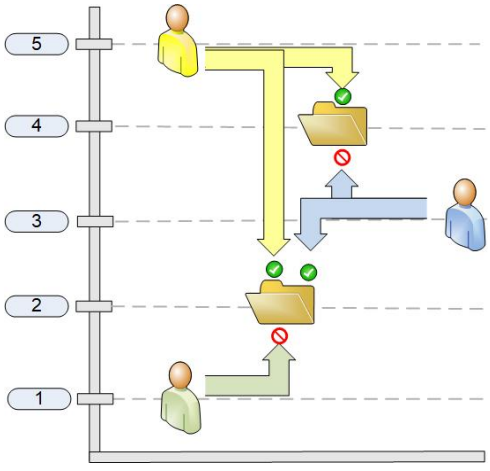
2. Расположите по порядку этапы формирования электронной цифровой подписи:
   a) Формирование подписи
   b) Генерация ключевой пары
   c) Проверка (верификация) подписи

Ответ
1. Генерация ключевой пары
2. Формирование подписи
3. Проверка (верификация) подписи

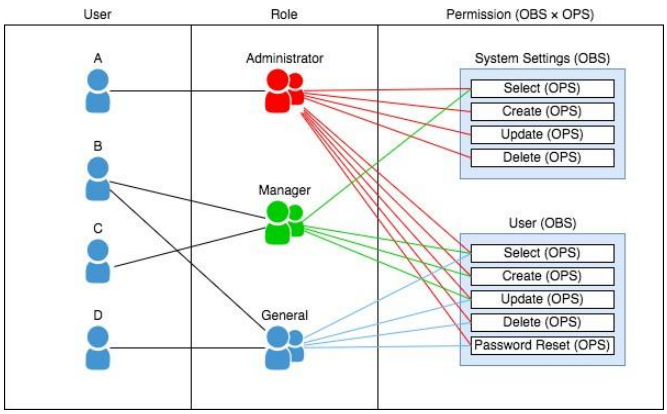
3. Установите соответствие:

а) мандатная модель управления;
б) управление доступом на основе правил
в) ролевая модель управления;

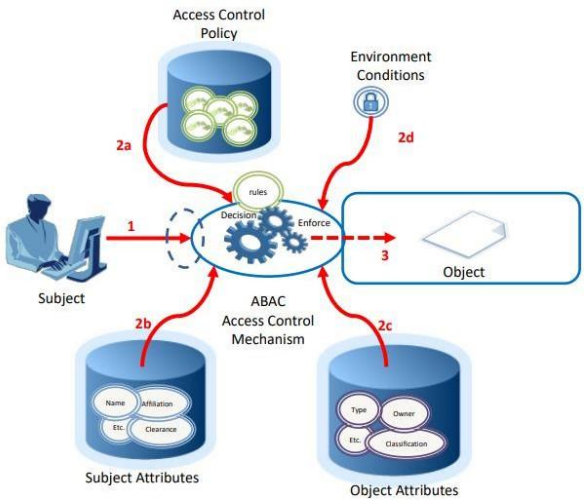
1.



2.



3.



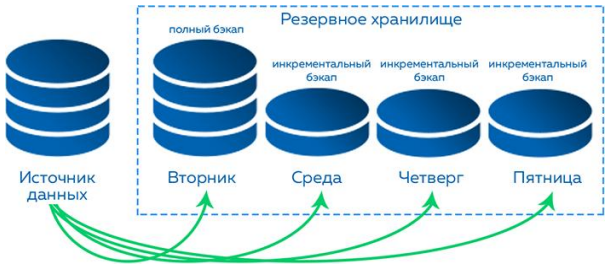
Ответ: 1-А; 2-В; 3-Б

4. Установите соответствие:

а) полное резервное копирование
б) дифференциальное резервное копирование
в) инкрементное резервное копирование

1.

2.



3.

Ответ: 1-А; 2-В; 3-Б

5. Установите соответствие:

1. это комплекс мероприятий, исключающих или ослабляющих возможность неконтролируемого выхода конфиденциальной информации за пределы контролируемой зоны за счет электромагнитных полей побочного характера и наводок
2. это комплекс мероприятий, исключающих или уменьшающих возможность неконтролируемого выхода конфиденциальной информации за пределы контролируемой зоны в виде производственных или промышленных отходов
3. это комплекс мероприятий, исключающих или уменьшающих возможность выхода конфиденциальной информации за пределы контролируемой зоны за счет акустических полей
4. это комплекс мероприятий, исключающих

а) защита информации от утечки по акустическому каналу
б) защита информации от утечки по визуально-оптическому каналу
в) защита информации от утечки по электромагнитным каналам
г) защита информации от утечки по материально-вещественному каналу

или уменьшающих возможность выхода конфиденциальной информации за пределы контролируемой зоны за счет распространения световой энергии

Ответ: 1-В; 2-Г; 3-А:4-Б

6. Установите соответствие:
   1. Симметричные криптосистемы
   2. Ассиметричные криптосистемы

а) ГОСТ
б) RSA
в) AES

Ответ: 1-а,в; 2-б

7. Установите соответствие:
   1. наука о скрытой передаче информации путем сохранения в тайне самого факта передачи
   2. наука, скрывающая содержимое секретного сообщения

а) криптография
б) стеганография

Ответ: 1-б; 2-а

8. Установите соответствие:
   1. средства, в которых программные (микропрограммные) и аппаратные части полностью взаимосвязаны и неразделимы
   2. электронные, электромеханические и другие устройства, непосредственно встроенные в блоки автоматизированной информационной системы или оформленные в виде самостоятельных устройств и сопрягающиеся с этими блоками
   3. средства защиты с помощью преобразования информации (например, шифрования)
   4. средства предназначены для выполнения логических и интеллектуальных функций защиты и включаются либо в состав программного обеспечения автоматизированной информационной системы, либо в состав средств, комплексов и систем аппаратуры контроля.
   5. предназначены для внешней охраны территории объектов, защиты компонентов автоматизированной информационной системы предприятия и реализуются в виде автономных устройств и систем

а) аппаратно-программные средства защиты
б) аппаратные средства защиты
в) криптографические средства защиты
г) программные средства защиты
д) физические средства защиты

Ответ: 1-а; 2-б; 3-в; 4-г; 5-д

9. Установите соответствие:

1. вид компьютерного вируса, функции, реализуемые программой, но не описанные в документации. Человек, знающий эту функцию, может заставить работать	а) червь б) логическая бомба в) троянский конь
2. участок программы, который реализует некоторые действия при наступлении определённых условий. Этим условием может быть, например, наступление какой-то даты или появление какого-то имени файла	
3. программа, внедряемая в систему, часто злонамеренно, и прерывающая ход обработки информации в системе, не искажает файлы данных, оставаясь необнаруженным, и затем самоуничтожается	

Ответ: 1-в; 2-б; 3-а;

10. Установите соответствие:

1. процесс изучения характеристик и слабых сторон системы, проводимый с использованием вероятностных расчётов, с целью определения ожидаемого ущерба в случае возникновения неблагоприятных событий. Определении степени приемлемости того или иного риска в работе системы	а) оценка риска б) анализ риска
2. метод анализа угроз и слабых сторон, известных и предполагаемых, позволяющий определить размер ожидаемого ущерба и степень его приемлемости для работы системы.	

Ответ: 1-б; 2-а;

Оценочные средства для промежуточной аттестации (экзамен)

Пример экзаменационного билета

ЭКЗАМЕНАЦИОННЫЙ БИЛЕТ № _

Теоретическая часть

Тест

1) Под угрозой безопасности информации в компьютерной системе (КС) понимают:

a) возможность возникновения на каком-либо этапе жизненного цикла КС такого ее состояния, при котором создаются условия для реализации угроз безопасности информации;

b) событие или действие, которое может вызвать изменение функционирования КС, связанное с нарушением защищенности обрабатываемой в ней информации;

c) действие, предпринимаемое нарушителем, которое заключается в поиске и использовании той или иной уязвимости.

2) Идентификация объекта– это:

a) одна из функций подсистемы защиты;

b) взаимное установление подлинности объектов, связывающихся между собой по линиям связи;

c) сфера действий пользователя и доступные ему ресурсы КС.

3) Для чего создается система разграничения доступа к информации:

a) для защиты информации от НСД;

b) для осуществления НСДИ;

c) определения максимального уровня конфиденциальности документа.

4) Аппаратно-программные средства криптографической защиты информации выполняют функции:

a) аутентификацию пользователя, разграничение доступа к информации, обеспечение целостности информации и ее защиты от уничтожения, шифрование и электронную цифровую подпись;

b) организовывают реализацию политики безопасности информации на этапе эксплуатации КС;

c) проверяют на отсутствие закладок приборов, устройств.

5) Возможные каналы утечки информации по классификации разделяют:

a) человек, линия связи;

b) коммутационное оборудование, человек;

c) человек, аппаратура, программа.

6) Асимметричная криптосистема предполагает использование

a) системы разграничения доступа;

b) двух ключей открытого и личного (секретного) ;

c) переносных носителей для хранения секретной информации.

7) Под компьютерным вирусом понимается:

a) программа имеющая доступ к файлам системы, и имеющая возможность работать с процессами системы;

b) автономно функционирующая программа, обладающая способностью к самостоятельному внедрению в тела других программ и последующему самовоспроизведению и самораспространению в информационно-вычислительных сетях и отдельных ЭВМ;

c) программа не имеющая доступ к файлам системы, и не имеющая возможность работать с процессами системы.

Практическое задание

Получить исходное сообщение, которое было зашифровано.
Для шифрования сообщения был применен комбинированный подход:
1) Перестановка (по методу Гамильтона), 5-2-1-6-4-8-7-3;
2) Обратимое XOR шифрование, 12345678901234567 89
Закодированное сообщение: ЯШоШШБЯЦРБФпЫйиЬ

Критерии и шкала оценивания по оценочному средству промежуточный контроль («экзамен»)

Шкала оценивания (интервал баллов)	Критерий оценивания
отлично (5)	Студент глубоко и в полном объёме владеет программным материалом. Грамотно, исчерпывающе и логично его излагает в устной или письменной форме. При этом знает рекомендованную литературу, проявляет творческий подход в ответах на вопросы и правильно обосновывает принятые решения, хорошо владеет умениями и навыками при выполнении практических задач.
хорошо (4)	Студент знает программный материал, грамотно и по сути излагает его в устной или письменной форме, допуская незначительные неточности в утверждениях, трактовках, определениях и категориях или незначительное количество ошибок. При этом владеет необходимыми умениями и навыками при выполнении практических задач.
удовлетворительно (3)	Студент знает только основной программный материал, допускает неточности, недостаточно чёткие формулировки, непоследовательность в ответах, излагаемых в устной или письменной форме. При этом недостаточно владеет

	умениями и навыками при выполнении практических задач. Допускает до 30% ошибок в излагаемых ответах.
неудовлетворительно (2)	Студент не знает значительной части программного материала. При этом допускает принципиальные ошибки в доказательствах, в трактовке понятий и категорий, проявляет низкую культуру знаний, не владеет основными умениями и навыками при выполнении практических задач. Студент отказывается от ответов на дополнительные вопросы

Лист изменений и дополнений

№ п/п	Виды дополнений и изменений	Дата и номер протокола заседания кафедры (кафедр), на котором были рассмотрены и одобрены изменения и дополнения	Подпись (с расшифровкой) заведующего кафедрой (заведующих кафедрами)