МИНИСТЕРСТВО НАУКИ И ВЫСШЕГО ОБРАЗОВАНИЯ
РОССИЙСКОЙ ФЕДЕРАЦИИ

Федеральное государственное бюджетное образовательное учреждение
высшего образования
«Луганский государственный университет
имени Владимира Даля»
(ФГБОУ ВО «ЛГУ им. В. Даля»)

Краснодонский факультет инженерии и менеджмента (филиал)
Кафедра информационных технологий и транспорта

УТВЕРЖДАЮ:
Директор
_____ Панайотов К.К.
(подпись)
«21» апреля 2023 года

РАБОЧАЯ ПРОГРАММА УЧЕБНОЙ ДИСЦИПЛИНЫ

По дисциплине Управление информационной безопасностью
(название дисциплины по учебному плану)

По направлению подготовки 38.04.05 Бизнес-информатика
(код, название без кавычек)

Магистерская программа Бизнес-аналитика

Краснодон 2023

Лист согласования РПУД

Рабочая программа учебной дисциплины «Управление информационной безопасностью» по направлению подготовки 38.04.05 – Бизнес-информатика, магистерская программа «Бизнес-аналитика» – 36 с.

Рабочая программа учебной дисциплины «Управление информационной безопасностью» разработана в соответствии с Федеральным государственным образовательным стандартом высшего образования по направлению подготовки 38.04.05 Бизнес-информатика (утвержденный приказом Министерства образования и науки Российской Федерации от 12 августа 2020 года № 990)

СОСТАВИТЕЛЬ (СОСТАВИТЕЛИ):

к.т.н. доц. Панайотов К.К

(ученая степень, ученое звание, должность фамилия, инициалы)

Рабочая программа дисциплины утверждена на заседании кафедры информационных технологий и транспорта «15» марта 2023 г., протокол № 7.

Заведующий кафедрой _____ Бихдрикер А.С.

Рекомендована на заседании учебно-методической комиссии факультета «20» марта 2023 г., протокол № 8.

Председатель учебно-методической комиссии факультета _____ Замота О.Н.

Структура и содержание дисциплины

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

Основной целью образования по дисциплине «Управление информационной безопасностью» являются получение обучающимися знаний, умений и навыков, необходимых и достаточных для обладания профессиональными компетенциями для последующей успешной организационно-управленческой и консалтинговой деятельности в сфере управления информационной безопасностью ИТ-инфраструктуры предприятия.

К задачам дисциплины относятся: приобретение теоретических знаний в области современных средств, методов и технологий обеспечения информационной безопасности информационных систем; формирование практических навыков в организации работ по обеспечению информационной безопасности на предприятиях.

2. Место дисциплины в структуре ООП ВО

Дисциплина Б1.О.08 "Управление информационной безопасностью" 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;

– стандарты, регламенты и инструкции управления системой обеспечения информационной безопасности предприятия;

– основные меры, направленные на обеспечение информационной безопасности на различных уровнях деятельности современного предприятия;

– перспективы развития технологий обеспечения информационной безопасности;

умения:

– анализировать и выбирать адекватные модели информационной безопасности;

– использовать знания о современной методологии управления ИБ для разработки реальных методов формирования защиты информационной инфраструктуры;

– применять методы формирования защиты информационной инфраструктуры для формирования и применения политик ИБ предприятия для эффективного управления процессами, работами и процедурами обеспечения ИБ;

– использованием современных инструментальных средств анализа рисков и разработки политики ИБ;

навыки:

– применять на практике международные и российские профессиональные стандарты информационной безопасности;

– базовыми навыками построения и управления систем защиты информации;

– навыками разработки концепции, программы, политики информационной безопасности предприятия;

– применять современные парадигмы и методологии, инструментальные средства реализации информационной безопасностью;

– организацией и проведение аудита ИБ.

Содержание дисциплины предполагает наличие базовых знаний в области информатики, информационных систем и технологий, моделирования бизнес-процессов, правового обеспечения деятельности.

3. Требования к результатам освоения содержания дисциплины

Код и наименование компетенции	Индикаторы достижений компетенции (по реализуемой дисциплине)	Перечень планируемых результатов
ОПК-2 Способен учитывать конкретные условия выполняемых задач и разрабатывать инновационные решения при управлении проектами и процессами в сфере	ОПК-2.1 Понимает специфику предметных областей, осуществляет управление информационной безопасностью	Знать: Основные стандарты и законодательство в области информационной безопасности; Стандарты, регламенты и инструкции управления системой обеспечения информационной безопасности предприятия; Перспективы развития технологий обеспечения информационной безопасности;
		Уметь: Анализировать и выбирать адекватные модели информационной безопасности; Использовать знания о современной методологии управления ИБ для разработки реальных методов формирования защиты информационной инфраструктуры;
		Владеть: Базовыми навыками построения и управления систем защиты информации; Навыками разработки концепции, программы, политики информационной безопасности предприятия;

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**
Общая учебная нагрузка (всего)	**180 (5 зач. ед)**		**180 (5 зач. ед)**
Обязательная контактная работа (всего) в том числе:	**56**		**12**
Лекции	28		6

Семинарские занятия	-		
Практические занятия	28		6
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)	**124**		**168**
Форма аттестации	экзамен		экзамен

4.2. Содержание разделов дисциплины

Тема 1. ВВЕДЕНИЕ В ДИСЦИПЛИНУ "УПРАВЛЕНИЕ ИНФОРМАЦИОННОЙ БЕЗОПАСНОСТЬЮ"

Цель и задачи дисциплины, ее роль и место в общей системе подготовки магистра. Понятие информационной безопасности. Важность и сложность проблемы информационной безопасности. Место информационной безопасности в национальной безопасности страны. Концепция информационной безопасности Российской Федерации/ Основные составляющие информационной безопасности. Информационная безопасность на уровне государства и предприятия.

Тема 2. ЗАКОНОДАТЕЛЬНАЯ ОСНОВА ИНФОРМАЦИОННОЙ БЕЗОПАСНОСТИ

Основные положения нормативной базы РФ и национальных стандартов в области информационной безопасности и защиты информации. Международные стандарты информационной безопасности и управления информационной безопасностью (ISO, ITIL, COBIT). Сертификация ПО.

***Тема 3.* ЗАЩИЩЕННАЯ ИНФОРМАЦИОННАЯ СИСТЕМА.**

Понятие "защищенная информационная система". Принципы защиты: доступность, целостность, конфиденциальность. Организационно-распорядительные документы в сфере информационной безопасности. Политика информационной безопасности. Архитектура безопасности. Управление доступом. Физическая защита. Управление изменениями. Управление конфигурациями. Управление инцидентами. Управление документацией. Резервирование.

Тема 4. УПРАВЛЕНИЯ РИСКАМИ ИНФОРМАЦИОННОЙ БЕЗОПАСНОСТИ

Виды защищаемой информации. Уязвимости, риски, угрозы. Классификация угроз информационной безопасности. Модель угроз и модель информационной безопасности. Обзор программных продуктов для оценки информационных рисков. Программный продукт CORAS.

Тема 5. ТЕХНОЛОГИИ И МЕТОДЫ РЕАЛИЗАЦИИ ИБ. КОМПЛЕКСНАЯ ЗАЩИТА ИНФОРМАЦИОННОЙ ИНФРАСТРУКТУРЫ

Правовые, программно-технические и организационно-экономические методы защиты информации. Парольная защита.

Криптографические методы защиты информации. ЭЦП. Защита информационной инфраструктуры от атак. Антивирусные средства защиты.

SIEM-системы (Security information and event management —«управление событиями и информационной безопасностью»).
DLS-системы (Data Leak Prevention).

Защита сети. Межсетевые экраны. VPN-туннели. Защита от Dos/DDos атак. Мониторинг и аудит безопасности информационной системы. Протоколирование.

4.3. Лекции

№ п/п	Название темы		Объем часов	
		Очная форма	Очно-заочная форма	заочная форма
1.	Тема 1. Введение в дисциплину "Управление информационной безопасностью"	2		0,5
2.	Тема 2. Законодательная основа информационной безопасности	4		0,5
3.	Тема 3. Защищенная информационная система.	6		2
4.	Тема 4. Управления рисками информационной безопасности	6		2
5.	Тема 5. Технологии и методы реализации ИБ. комплексная защита информационной инфраструктуры	10		3
Итого:		**28**		**8**

4.4. Практические (семинарские) занятия

№ п/п	Название темы	Объем часов		
		Очная форма	Очно-заочная форма	заочная форма
1.	Структура информационной безопасности современного предприятия	2		0,5
2.	Подготовка предварительного варианта концепции информационной безопасности компании. (Разработка корпоративной концепции информационной безопасности)	2		0,5
3.	Анализ рисков информационной безопасности. CORAS	2		0,5
4.	Анализ и управление рисками информационной безопасности. ГРИФ.	4		1
5.	Парольная защита	2		1
6.	Электронная цифровая подпись.	2		1
7.	Виртуальные частные сети. Создание VPN туннеля	4		1
8.	Политика информационной безопасности. КОНДОР	4		1
9.	Построение комплексной системы информационной защиты. DLS-системы	4		1
10.	Оценка надежности защитных механизмов ИБ	2		0,5
Итого:		**28**		**8**

4.6. Самостоятельная работа студентов

№ п/п	Название темы	Вид СРС	Объем часов		
			Очная форма	Очно-заочная форма	заочная форма
1.	Структура информационной безопасности современного предприятия	Выполнение задания по вариантам. Оформление отчета	6		6
2.	Подготовка предварительного варианта концепции информационной безопасности компании. (Разработка корпоративной концепции информационной безопасности)	Выполнение задания по вариантам. Оформление отчета	8		8
3.	Анализ рисков информационной безопасности. CORAS	Выполнение задания по вариантам. Оформление отчета	10		12
4.	Анализ и управление рисками информационной безопасности. ГРИФ.	Выполнение задания по вариантам. Оформление отчета	10		12
5.	Парольная защита	Выполнение задания по вариантам. Оформление отчета	4		6
6.	Электронная цифровая подпись.	Выполнение задания по вариантам. Оформление отчета	6		8
7.	Виртуальные частные сети. Создание VPN туннеля	Выполнение задания по вариантам. Оформление отчета	10		12
8.	Политика информационной безопасности. КОНДОР	Выполнение задания по вариантам. Оформление отчета	12		14
9.	Построение комплексной системы информационной защиты. DLS-системы	Выполнение задания по вариантам. Оформление отчета	12		14
10.	Оценка надежности защитных механизмов ИБ	Выполнение задания по вариантам. Оформление отчета	10		12
11	Подготовка к зачету/экзамену	Повтор теоретического материалы.	36		40
Итого:			**124**		**144**

4.7. Курсовые работы/проекты по дисциплине «Управление информационной безопасностью» 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. 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

2. 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

3. 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

4. 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

б) дополнительная литература:

1. 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

2. Ерохин, В. В. Безопасность информационных систем : Учебное пособие / В. В. Ерохин, Д. А. Погонышева, И. Г. Степченко. – Москва : "ФЛИНТА", "Наука", 2015. – 184 с. – ISBN 978-5-9765-1904-6. – EDN VSIOUN. — URL : https://www.elibrary.ru/download/elibrary_25788507_90414101.pdf

3. 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

4. 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

5. 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

6. 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

7. 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

в) методические указания:

1. 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.

2. 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.

3. 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.

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 «Управление информационной безопасностью» 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
«Управление информационной безопасностью»

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-2	Способен учитывать конкретные условия выполняемых и разрабатывать инновационные решения при управлении проектами процессами в сфере информационно-коммуникационных технологий	ОПК-2.1 Понимает специфику предметных областей, осуществляет управление информационной безопасностью	Тема 1. Введение в дисциплину "Управление информационной безопасностью"	1
				Тема 2. Законодательная основа информационной безопасности	1
				Тема 3. Защищенная информационная система.	1
				Тема 4. Управления рисками информационной безопасности	1
				Тема 5. Технологии и методы реализации ИБ. комплексная защита информационной инфраструктуры	1

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-2	ОПК-2.1	Знать: – основные стандарты и законодательство в области информационной безопасности; – стандарты, регламенты и инструкции управления системой обеспечения информационной безопасности предприятия; – перспективы развития технологий обеспечения информационной безопасности; Уметь: – анализировать и выбирать адекватные модели информационной безопасности; – использовать знания о современной методологии управления ИБ для разработки реальных методов формирования защиты информационной инфраструктуры; Владеть: – базовыми навыками построения и	Тема 1. Тема 2. Тема 3. Тема 4. Тема 5.	Устный опрос, контрольная работа (по вариантам), тесты

			управления систем защиты информации; – навыками разработки концепции, программы, политики информационной безопасности предприятия;		

Фонды оценочных средств по дисциплине
«Управление информационной безопасности»

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

1. Понятие информационной безопасности.
2. Виды защищаемой информации.
3. Перечислите составляющие информационной безопасности.
4. Приведите определение доступности информации.
5. Приведите определение целостности информации.
6. Приведите определение конфиденциальности информации.
7. Типы атак и угроз.
8. Внешние источники угроз
9. Внутренние источники угроз
10. Каналы утечки информации.
11. Стандарты информационной безопасности.
12. Управление информационной безопасности.
13. Политика информационной безопасности.
14. Основные методы обеспечения информационной безопасности.
15. Принципы построения защищенных систем.
16. Симметричные криптосистемы.
17. Ассиметричные криптосистемы.
18. Профилактика заражения вирусами. Поиск и удаление шпионских и рекламных модулей
19. Криптографические методы защиты.
20. Протоколы аутентификации. Слабости парольных протоколов аутентификации. Виды атак и угроз для протоколов аутентификации.
21. Протоколы электронной подписи. Общие понятия и определения. Виды атак и угроз для протоколов электронной подписи.
22. Показатели защищенности межсетевых экранов.
23. Классы защищенности межсетевых экранов.
24. Электронная цифровая подпись.
25. Архитектура системы безопасности ОС.
26. Дайте определение политики безопасности.
27. Какие сервисы безопасности включает технология виртуальных частных сетей?
28. Что такое "туннель" и технология его создания?
29. SIEM-системы.
30. DLS-системы.

31. Направления разработки политики безопасности.
32. Методология COBIT.
33. Анализ рисков информационной безопасности.
34. Инструментарий анализа анализ рисков информационной безопасности.
35. Мониторинг и аудит 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)

Провести анализ оценки рисков информационной безопасности предприятия (определенной сферы деятельности) на основе методики COBIT (с использованием программного инструментария CORAS).

Производственное предприятие расположено в отдельном 2-х этажном здании с одним центральным входом и одним запасным выходом. На каждом этаже есть большие окна, выходящие на южную и восточную стороны. Род занятий связан с передовыми технологиями. В структуре предприятия функционирует несколько подразделений, имеющих отдельные помещения.

В сеть через витую пару, оптоволокно, Wi-Fi и Bluetooth выходят не менее 10 стационарных компьютеров и несколько ноутбуков. Единый сервер обслуживает хранение рабочих файлов, базы данных предприятия, а также корпоративный сайт, доступный за пределами локальной сети. Интернет к зданию подводится по оптоволокну. Периферийные устройства: принтеры, факсы, телефоны.

Провести оценку анализа рисков информационной безопасности. Указать объекты защиты и возможные угрозы. Присвоить каждой угрозе свою оценку по 10 бальной шкале (10 максимальная угроза). Предложить средства защиты. Выполнить используя методологию COBIT и программный продукт CORAS.

Критерии и шкала оценивания по оценочному средству «контрольная работа (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

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. 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

3. 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

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

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

6. 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

7. 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

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. 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.

10. Для чего создается система разграничения доступа к информации:

a) для защиты информации от НСД;

b) для осуществления НСДИ;

c) определения максимального уровня конфиденциальности документа.

11. Процедуру установки сфер действия пользователя и доступные ему ресурсы КС называют:

a) аутентификацией;

b) авторизацией;

c) идентификация.

12. Искусственные угрозы исходя из их мотивов разделяются на:

a) косвенные и непосредственные;

b) несанкционированные и санкционированные.

c) непреднамеренные и преднамеренные;

13. Аутентификация – это:

a) подтверждение подлинности;

b) предоставлением полномочий;

c) цифровая подпись.

14. 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.

15. 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.

16. 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.

17. 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.

18. 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).

19. 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;

20. 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.

21. 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.

22. 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

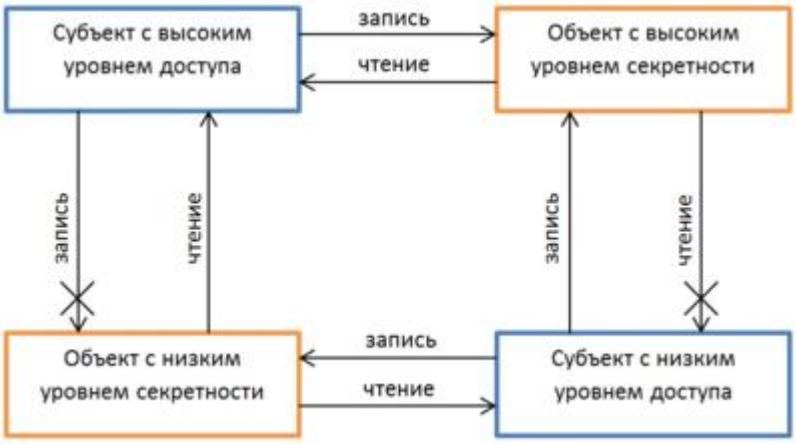
23. Укажите возможные методы восстановления пароля в программах вкрытия паролей

a) Перебор по маске
b) Атака по словарю
c) Прямой перебор
d) По электронной почте

24. Для чего служат сети VPN (укажите правильный ответ)?

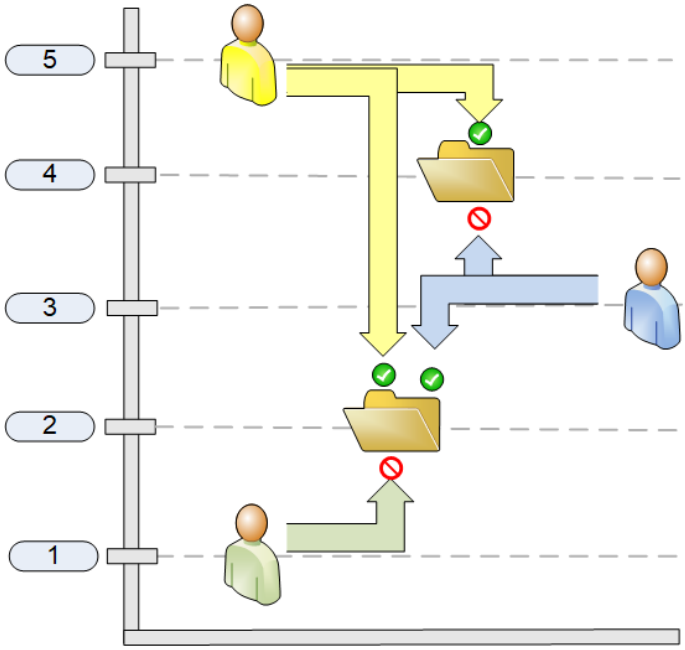
a) для обеспечения соединения трёх видов: узел-узел, узел-сеть и сеть-сеть (в зависимости от применяемых протоколов)
b) для обеспечения сетевых соединений поверх другой сети (например, Интернет)
c) для улучшения безопасности локальной сети
d) для увеличения быстродействия локальной сети

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



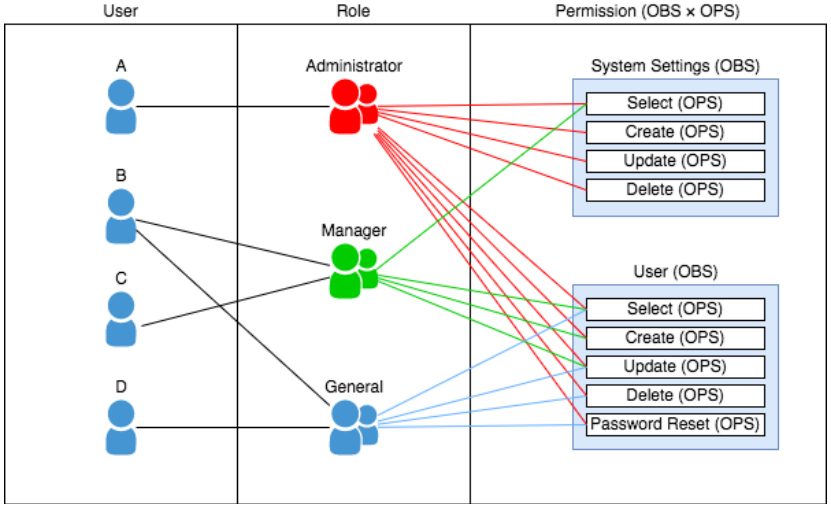
a) **Модель Белла-Лападулы**
b) Модель Фостера-Стюарта
c) Модель Бокса-Дженкинса

26. Схема какой модели управления доступом представлена на рисунке?



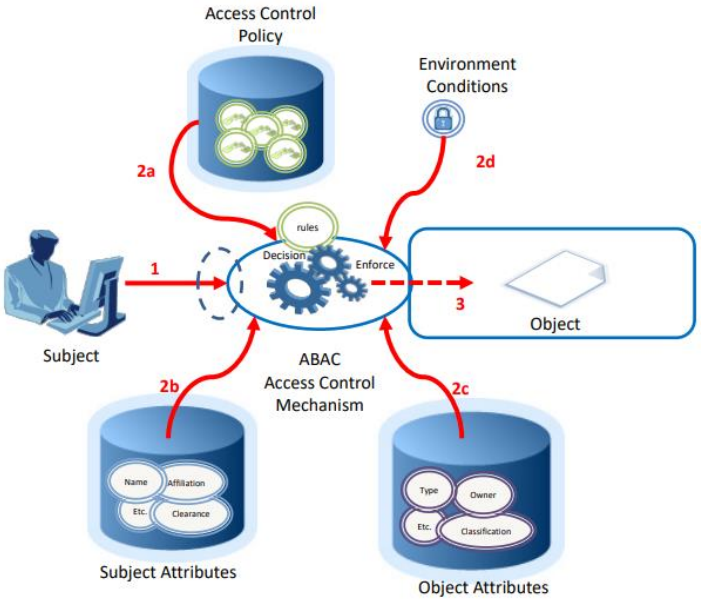
a) дискреционная модель управления;
b) мандатная модель управления;
c) ролевая модель управления;
d) управление доступом на основе правил

27. 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

28. 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

29. 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

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

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

32. Какой метод создания резервных копий представлен на рисунке?

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

33. Какой метод создания резервных копий представлен на рисунке?

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

34. Какой метод создания резервных копий представлен на рисунке?

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

35. 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

36. Кто в конечном счете несет ответственность за гарантии того, что данные классифицированы и защищены?
a) Владельцы данных
b) Пользователи
c) Администраторы
d) Руководство

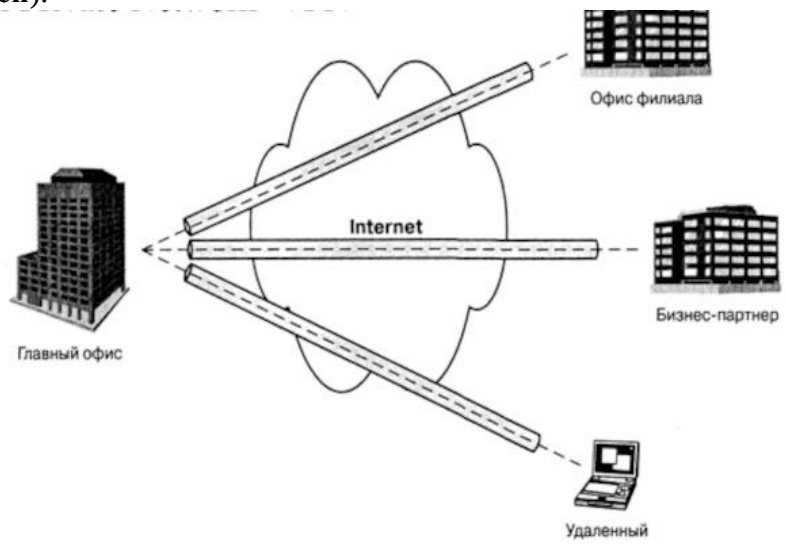
37. Что такое CobiT и как он относится к разработке систем информационной безопасности и программ безопасности?
a) Список стандартов, процедур и политик для разработки программы безопасности
b) Текущая версия ISO 27799
c) Открытый стандарт, определяющий цели контроля
d) Структура, которая была разработана для снижения внутреннего мошенничества в компаниях

Задания открытого типа

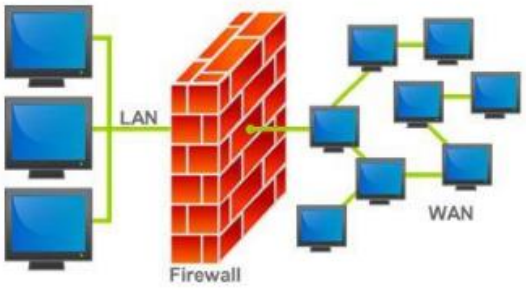
1. Состояние защищенности жизненно важных интересов личности, общества, государства в информационной сфере (среде)_____ (**информационная безопасность**)

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

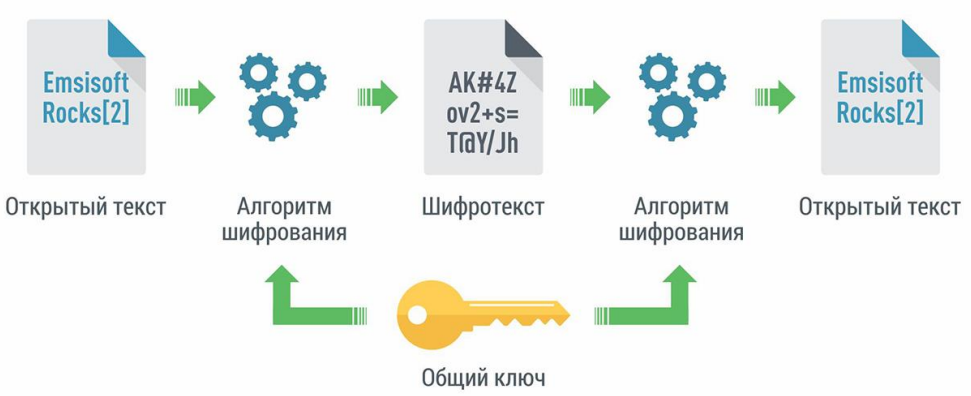
3. Какая технология построения сетей изображена на рисунке ниже. _____ (**VPN/виртуальных сетей**).



4. 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**)

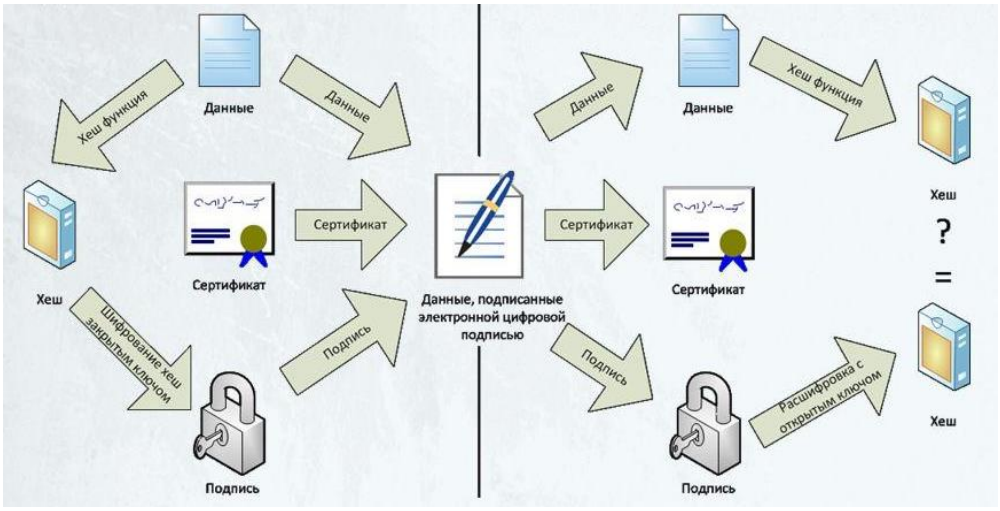


5. Схема какого метода закрытия информации представлена на рисунке? _____(**Симметричное шифрование/симметричного**)



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

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



8. Представление информации в виде условных сигналов с целью автоматизации ее хранения, обработки, передачи и т.д. _____ (**кодирование**).

9. 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**)

10. Потенциально возможное событие, действие, процесс или явление, которое может причинить ущерб чьих-нибудь данных, называется _____ (**угроза**)

11. 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**)

12. Метод пароля и его модификация, метод вопрос-ответ, метод секретного алгоритма - это методы _____ (**аутентификации**)

13. Совокупность документированных правил, процедур, практических приемов или руководящих принципов в области безопасности информации, которыми руководствуется организация в своей деятельности называется _____(**политикой безопасности**)

14. 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**)

15. 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**)

16. Состояние защищенности жизненно важных интересов личности, общества и государства от внутренних и внешних угроз — это _____ (**безопасность**)

17. Сведения о фактах, событиях и обстоятельствах жизни гражданина, позволяющие идентифицировать его личность _____ (**персональные данные**)

18. Система штатных органов управления и организационных формирований, предназначенных для обеспечения безопасности информации предприятия _____(**служба безопасности**)

19. Сколько текстовой информации может быть скрыто методами стеганографии в цветной фотографии, сделанной 3-х мегапиксельной камерой мобильного телефона?

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

21. Поддельные сообщения от имени банков или финансовых компаний, целью которых является сбор логинов, паролей и пин-кодов пользователей называется _____ (**фишинг**)

22. Одиночная **атаки**, в котором мошенники нападают с целью вызвать перегрузку подсистемы сервиса, путём отправки максимального количества трафика жертве. _____ (**DoS-атака**)

23. На каком уровне эталонной семиуровневой модели может быть реализовано туннелирование? _____ (**сетовом/сетевом уровне**)

24. Профессиональные взломщики защиты компьютерных программ и создатели компьютерных вирусов _____ (**хакеры**)

25. 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**)

26. Неправомерный доступ к компьютерной информации, если это деяние повлекло уничтожение, блокирование, модификацию либо копирование информации, нарушение работы ЭВМ, системы ЭВМ или их сети, – наказывается _____ (**штрафом**)

27. Кто является основным ответственным за определение уровня классификации информации? _____ (**владелец**)

28. Всестороннее обследование, позволяющее оценить текущее состояние информационной безопасности организации и спланировать дальнейшие шаги по повышению уровня защищенности — это _____информационной безопасности (**аудит**)

29. Процесс наблюдения, анализа и оценки систем и сетей на предмет возможных угроз, вредоносного кода, уязвимостей и нарушений политик безопасности — это _____информационной безопасности (**мониторинг**)

30. Возможность того, что данная угроза сможет воспользоваться уязвимостью актива или группы активов и тем самым нанесет ущерб организации — это _____информационной безопасности (**риск**).

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

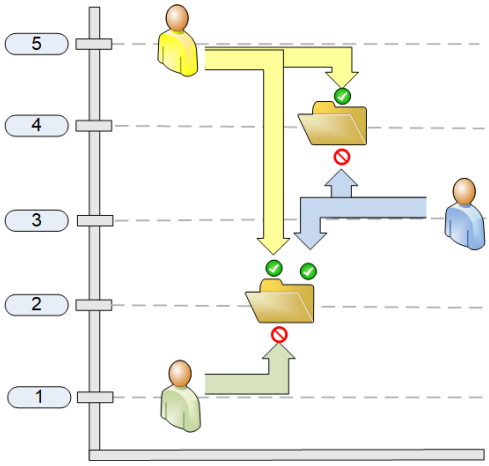
2. Расположите по порядку этапы формирования электронной цифровой подписи:
a) Формирование подписи
b) Генерация ключевой пары
c) Проверка (верификация) подписи

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

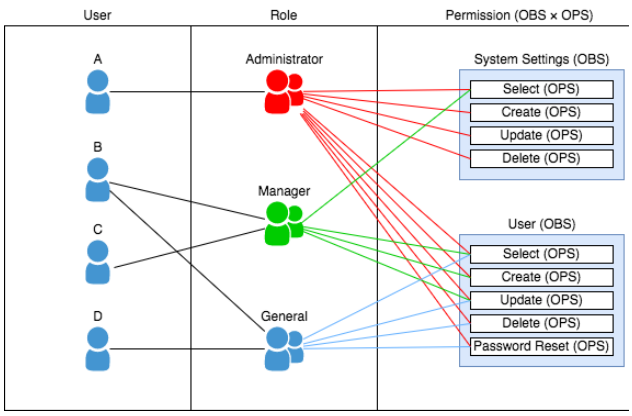
3. Установите соответствие:

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

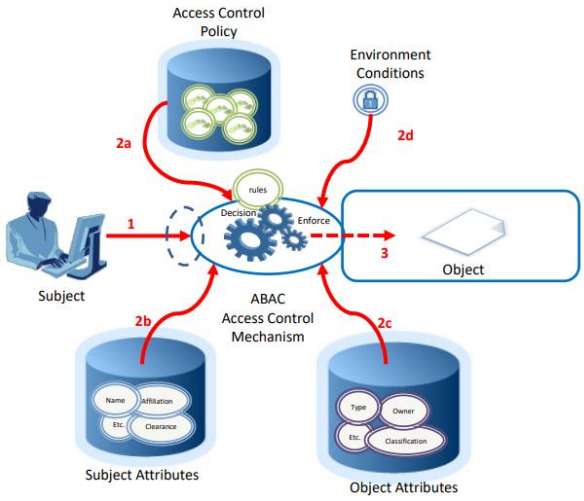
1.



2.



3.



Ответ: 1-А; 2-В; 3-Б

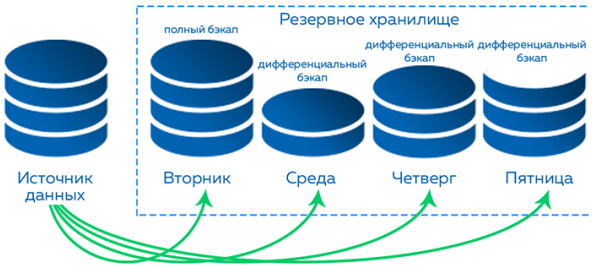
4. Установите соответствие:

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

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

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
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

а) червь
б) логическая бомба
в) троянский конь

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

2. метод анализа угроз и слабых сторон, известных и предполагаемых, позволяющий определить размер ожидаемого ущерба и степень его приемлемости для работы системы.

а) оценка риска
б) анализ риска

Ответ: 1-б; 2-а;

11. Установите соответствие:

1. SIEM-системы
2. DLS-система

а) программный продукт для предотвращения утечек конфиденциальных данных в корпоративной сети
б) решение, которое позволяет организациям обнаруживать, анализировать и устранять угрозы безопасности раньше, чем они нанесут ущерб бизнесу

Ответ: 1-б; 2-а;

12. Установите соответствие:

1. Пиктограмма "Уязвимость" в CORAS
2. Пиктограмма "Риск" в CORAS
3. Пиктограмма "Противодействие угрозам" в CORAS
4. Пиктограмма "Инцидент" в CORAS
5. Пиктограмма "Владелец информации" в CORAS

а) 
б) 
в) 
г) 
д) 

Ответ: 1-б; 2-а; 3-в 4-г 5-д

Оценочные средства для промежуточной аттестации (экзамен)

1. Научно-технический прогресс и этапы развития защиты информации.
2. Система защиты информации.
3. Современная концепция информационной безопасности.
4. Цели защиты информации.
5. Законодательство в области защиты информации.
6. Требования к организации защиты информации, обязанности и права субъектов.
7. Государственная система защиты информации.

8. Анализ угроз информационной безопасности.
9. Классификация видов угроз информационной безопасности по различным признакам.
10. Основные положения теории информационной безопасности информационных систем.
11. Формальные модели безопасности.
12. Политики безопасности информационных систем.
13. Домены безопасности.
14. Федеральные критерии безопасности информационных технологий.
15. Профиль защиты.
16. Ядро безопасности, как совокупность аппаратных, программных и специальных компонент вычислительной системы.
17. Роль стандартов информационной безопасности.
18. Квалификационный анализ уровня безопасности.
19. Классификация компьютерных вирусов по среде обитания, поражаемой операционной системе, особенностям алгоритма работы, деструктивным возможностям.
20. Жизненный цикл и среда обитания компьютерных вирусов.
21. Структура антивирусной программы.
22. Политика безопасности при доступе в сети общего пользования.
23. Средства криптографической защиты информации (СКЗИ).
24. Идентификация и аутентификация.
25. Парольные схемы аутентификации.
26. Симметричные схемы аутентификации субъекта.
27. Шифрование информации с секретным ключом (симметричные алгоритмы).
28. Режимы шифрования (электронная кодовая книга, сцепление блоков шифра, обратная связь по шифротексту, обратная связь по выходу).
29. Стандарты шифрования (DES, ГОСТ 28147-89).
30. Сравнительный анализ симметричных алгоритмов.
31. Шифрование информации с открытым ключом.
32. Сравнение симметричных и несимметричных алгоритмов шифрования.
33. Проблемная область формирования информационной безопасности.
34. Правовые основы реализации информационной безопасности.
35. Защита интеллектуальной собственности как одна из форм защиты информации.
36. Использование принципа системного подхода при анализе информационной защищенности предприятия.
37. Методологии и инструменты формирования информационной защиты предприятия.
38. Современные международные стандарты реализации ИБ.
39. Принципы построения системы ИБ.
40. Модели «нарушителя» и модели угроз ИБ.
41. Разработка системы качественных и количественных показателей для оценки защищенности информационной инфраструктуры.
42. Особенности информационных рисков, современные стандарты и программные продукты для оценки информационных рисков.
43. Система стандартов для реализации информационной безопасности предприятия.
44. Сервисы информационной защиты.
45. Программно-аппаратные и технические средства защиты информационных ресурсов.
46. Комплексная система информационной защиты.

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

9. Особенности организации обучения для лиц с ограниченными возможностями здоровья и инвалидов

При необходимости рабочая программа учебной дисциплины может быть адаптирована для обеспечения образовательного процесса инвалидов и лиц с ограниченными возможностями здоровья, в том числе с применением электронного обучения и дистанционных образовательных технологий.

Для этого требуется заявление студента (его законного представителя) и заключение психолого-медико-педагогической комиссии (ПМПК). В случае необходимости обучающимся из числа лиц с ограниченными возможностями здоровья (по заявлению обучающегося), а для инвалидов также в соответствии с индивидуальной программой реабилитации инвалида могут предлагаться следующие варианты восприятия учебной информации с учетом их индивидуальных психофизических особенностей:

– создание текстовой версии любого нетекстового контента для его возможного преобразования в альтернативные формы, удобные для различных пользователей;

– создание контента, который можно представить в различных видах без потери данных или структуры, предусмотреть возможность масштабирования текста и изображений без потери качества, предусмотреть доступность управления контентом с клавиатуры;

– создание возможностей для обучающихся воспринимать одну и ту же информацию из разных источников, например, так, чтобы лица с нарушениями слуха получали информацию визуально, с нарушениями зрения – аудиально;

– применение программных средств, обеспечивающих возможность освоения навыков и умений, формируемых дисциплиной (модулем), за счёт альтернативных способов, в том числе виртуальных лабораторий и симуляционных технологий;

– применение электронного обучения, дистанционных образовательных технологий для передачи информации, организации различных форм интерактивной контактной работы обучающегося с преподавателем, в том числе вебинаров, которые могут быть использованы для проведения виртуальных лекций с возможностью взаимодействия всех участников дистанционного обучения, проведения семинаров, выступления с докладами и защиты выполненных работ, проведения тренингов, организации коллективной работы;

– применение электронного обучения, дистанционных образовательных технологий для организации форм текущего и промежуточного контроля;

– увеличение продолжительности сдачи обучающимся инвалидом или лицом с ограниченными возможностями здоровья форм промежуточной аттестации по отношению к установленной продолжительности их сдачи:

– продолжительность сдачи зачёта или экзамена, проводимого в письменной форме, – не более чем на 90 минут;

– продолжительность подготовки обучающегося к ответу на зачёте или экзамене, проводимом в устной форме, – не более чем на 20 минут; – продолжительность выступления обучающегося при защите курсовой работы – не более чем на 15 минут.

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)