Минобрнауки России

ФЕДЕРАЛЬНОЕ ГОСУДАРСТВЕННОЕ БЮДЖЕТНОЕ ОБРАЗОВАТЕЛЬНОЕ УЧРЕЖДЕНИЕ ВЫСШЕГО ОБРАЗОВАНИЯ

«ВОРОНЕЖСКИЙ ГОСУДАРСТВЕННЫЙ УНИВЕРСИТЕТ»

(ФГБОУ ВО «ВГУ»)

УТВЕРЖДАЮ

Заведующий кафедрой

Сирота Александр Анатольевич

Кафедра технологий обработки и защиты информации

03.05.2023

РАБОЧАЯ ПРОГРАММА УЧЕБНОЙ ДИСЦИПЛИНЫ

Б1.О.45 Комплексное обеспечение защиты информации объекта информатизации

1. Код и наименование направления подготовки/специальности:

10.03.01 Информационная безопасность

2. Профиль подготовки/специализация:

Безопасность компьютерных систем

3. Квалификация (степень) выпускника:

Бакалавриат

4. Форма обучения:

Очная

5. Кафедра, отвечающая за реализацию дисциплины:

Кафедра технологий обработки и защиты информации

6. Составители программы:

Иванков Александр Юрьевич, к.ф.-м.н., доцент

7. Рекомендована:

№7 от 03.05.2023

8. Учебный год:

2026-2027

9.Цели и задачи учебной дисциплины:

Изучение основ и овладение практическими навыками планирования, развертывания и поддержания комплекса регламентов и процедур, направленных на минимизацию рисков нарушения информационной безопасности на объектах информатизации.
Основные задачи дисциплины:
- формирование системного подхода к оценке угроз безопасности информации на объектахинформатизации и комплексного обеспечения их защиты;
- освоение студентами положений и требований, современных нормативнометодическихдокументов, регламентирующих меры, обеспечивающие информационную безопасность на объектах информатизации;
- формирование представления о процедурах подготовки объектов информатизации кэксплуатации, включая вопросы применения мер и средств защиты информации и аттестации объектов;
- овладение практическими навыками разработки системы документов, регламентирующихтребования и меры, обеспечивающие информационную безопасность на

объектах информатизации.

10. Место учебной дисциплины в структуре ООП:

Блок Б1.О обязательные дисциплины.
Входные знания в области физики, распространения сигналов, основ информационной безопасности, организационного и правового обеспечения информационной безопасности, программно-аппаратных средств защиты информации.

11. Планируемые результаты обучения по дисциплине/модулю (знания, умения, навыки), соотнесенные с планируемыми результатами освоения образовательной программы (компетенциями выпускников) и индикаторами их достижения:

Код и название компетенции	Код и название индикатора компетенции	Знания, умения, навыки
ОПК-8 Способен осуществлять подбор, изучение и обобщение научно-технической литературы, нормативных и методических документов в целях решения задач профессиональной деятельности;	ОПК-8.1 знает принципы и порядок работы информационно-справочных систем	знает принципы и порядок работы информационносправочных систем
ОПК-8 Способен осуществлять подбор, изучение и обобщение научно-технической литературы, нормативных и методических документов в целях решения задач профессиональной деятельности;	ОПК-8.2 знает способы поиска и обработки информации, методы работы с научной информацией, принципы и правила построения суждений и оценок	знает способы поиска и обработки информации, методы работы с научной информацией, принципы и правила построения суждений и оценок
ОПК-8 Способен осуществлять подбор, изучение и обобщение научно-технической литературы, нормативных и методических документов в целях решения задач профессиональной деятельности;	ОПК-8.3 умеет обобщать, анализировать и систематизировать научную информацию в области информационной безопасности	умеет обобщать, анализировать и систематизировать научную информацию в области информационной безопасности

Код и название компетенции	Код и название индикатора компетенции	Знания, умения, навыки
ОПК-8 Способен осуществлять подбор, изучение и обобщение научно-технической литературы, нормативных и методических документов в целях решения задач профессиональной деятельности;	ОПК-8.4 умеет различать факты, интерпретации, оценки и аргументированно отстаивать свою позицию в процессе коммуникации	умеет различать факты, интерпретации, оценки и аргументированно отстаивать свою позицию в процессе коммуникации
ОПК-8 Способен осуществлять подбор, изучение и обобщение научно-технической литературы, нормативных и методических документов в целях решения задач профессиональной деятельности;	ОПК-8.5 умеет пользоваться информационно-справочными системами	умеет пользоваться информационносправочными системами
ОПК-8 Способен осуществлять подбор, изучение и обобщение научно-технической литературы, нормативных и методических документов в целях решения задач профессиональной деятельности;	ОПК-8.6 владеет навыком составления и оформления реферата по результатам обзора научно-технической литературы, нормативных и методических документов	владеет навыком составления и оформления реферата по результатам обзора научнотехнической литературы, нормативных и методических документов
ОПК-12 Способен проводить подготовку исходных данных для проектирования подсистем, средств обеспечения защиты информации и для технико-экономического обоснования соответствующих проектных решений;	ОПК-12.1 знает принципы формирования политики информационной безопасности в информационных системах;	знает принципы формирования политики информационной безопасности в информационных системах

Код и название компетенции	Код и название индикатора компетенции	Знания, умения, навыки
ОПК-12 Способен проводить подготовку исходных данных для проектирования подсистем, средств обеспечения защиты информации и для технико-экономического обоснования соответствующих проектных решений;	ОПК-12.2 знает принципы организации информационных систем в соответствии с требованиями по защите информации;	знает принципы организации информационных систем в соответствии с требованиями по защите информации
ОПК-12 Способен проводить подготовку исходных данных для проектирования подсистем, средств обеспечения защиты информации и для технико-экономического обоснования соответствующих проектных решений;	ОПК-12.3 знает требования Единой системы конструкторской документации и Единой системы программной документации при разработке технической документации;	знает требования Единой системы конструкторской документации и Единой системы программной документации при разработке технической документации
ОПК-12 Способен проводить подготовку исходных данных для проектирования подсистем, средств обеспечения защиты информации и для технико-экономического обоснования соответствующих проектных решений;	ОПК-12.4 знает основные этапы процесса проектирования и общие требования к содержанию проекта;	знает основные этапы процесса проектирования и общие требования к содержанию проекта
ОПК-12 Способен проводить подготовку исходных данных для проектирования подсистем, средств обеспечения защиты информации и для технико-экономического обоснования соответствующих проектных решений;	ОПК-12.5 умеет определять информационную инфраструктуру и информационные ресурсы организации, подлежащие защите;	умеет определять информационную инфраструктуру и информационные ресурсы организации, подлежащие защите

Код и название компетенции	Код и название индикатора компетенции	Знания, умения, навыки
ОПК-12 Способен проводить подготовку исходных данных для проектирования подсистем, средств обеспечения защиты информации и для технико-экономического обоснования соответствующих проектных решений;	ОПК-12.6 умеет анализировать показатели качества и критерии оценки систем и отдельных методов и средств защиты информации;	умеет анализировать показатели качества и критерии оценки систем и отдельных методов и средств защиты информации
ОПК-12 Способен проводить подготовку исходных данных для проектирования подсистем, средств обеспечения защиты информации и для технико-экономического обоснования соответствующих проектных решений;	ОПК-12.7 умеет формировать требования и разрабатывать внешние спецификации для разрабатываемого программного обеспечения;	умеет формировать требования и разрабатывать внешние спецификации для разрабатываемого программного обеспечения
ОПК-12 Способен проводить подготовку исходных данных для проектирования подсистем, средств обеспечения защиты информации и для технико-экономического обоснования соответствующих проектных решений;	ОПК-12.8 умеет оценивать информационные риски в автоматизированных системах;	умеет оценивать информационные риски в автоматизированных системах
ОПК-12 Способен проводить подготовку исходных данных для проектирования подсистем, средств обеспечения защиты информации и для технико-экономического обоснования соответствующих проектных решений;	ОПК-12.9 умеет разрабатывать основные показатели технико-экономического обоснования соответствующих проектных решений;	умеет разрабатывать основные показатели техникоэкономического обоснования соответствующих проектных решений

12. Объем дисциплины в зачетных единицах/час:

4/144

Форма промежуточной аттестации:

Экзамен

13. Трудоемкость по видам учебной работы

Вид учебной работы	Семестр 8	Всего
Аудиторные занятия	72	72
Лекционные занятия	36	36
Практические занятия		0
Лабораторные занятия	36	36
Самостоятельная работа	36	36
Курсовая работа		0
Промежуточная аттестация	36	36
Часы на контроль	36	36
Всего	144	144

13.1. Содержание дисциплины

п/п	Наименование раздела дисциплины	Содержание раздела дисциплины	Реализация раздела дисциплины с помощью онлайн-курса, ЭУМК
Лекции			
1	Защита информации на объекте информатизации, основные положения	1. Защита конфиденциальности, целостности, доступности. Средства и меры защиты. Комплексное обеспечение защиты информации. 2. Лицензирование деятельности в области защиты информации. Сертификация средств защиты информации.	Создан электронный онлайн - курс, размещены материалы к лекциям и лабораторным занятиям.
2	Технические каналы утечки информации	3. Технические каналы утечки информации. Классификация, причины и источники образования. 4. Радиоканалы. Акустические каналы. Электрические каналы. 5. Линии связи. Визуально-оптические каналы. 6. Материально-вещественные каналы. 7. Методы и средства несанкционированного получения информации по техническим каналам.	Создан электронный онлайн - курс, размещены материалы к лекциям и лабораторным занятиям.

п/п	Наименование раздела дисциплины	Содержание раздела дисциплины	Реализация раздела дисциплины с помощью онлайн-курса, ЭУМК
3	Угрозы несанкционированного доступа к информации в компьютерных системах	8. Базовая модель угроз безопасности персональных данных при их обработке в информационных системах персональных данных (выписка). (http://fstec.ru/component/attachments/download/289). Банк данных угроз безопасности информации ФСТЭК России, http://bdu.fstec.ru/. 9. Методика определения угроз безопасности информации в информационных системах, проект, ФСТЭК России, май 2015 г., (http://fstec.ru/component/attachments/download/812). 10. Меры защиты информации в государственных информационных системах. Методические документы ФСТЭК России. (http://fstec.ru/component/attachments/download/675). 11. Методика моделирования угроз безопасности информации. Методические документы ФСТЭК России. (http://fstec.ru/component/attachments/download/2727).	Создан электронный онлайн - курс, размещены материалы к лекциям и лабораторным занятиям.
4	Методы и средства защиты информации на объекте информатизации	12. Правовые и организационные методы и средства защиты информации на объекте информатизации. 13. Физические, технические методы и средства защиты информации на объекте информатизации. 14. Программные методы защиты информации на объекте информатизации. 15. Криптографические средства защиты информации.	Создан электронный онлайн - курс, размещены материалы к лекциям и лабораторным занятиям.
5	Контроль эффективности защиты информации на объекте информатизации	16. Документы, необходимые для ввода объекта информатизации в эксплуатацию. 17. Аттестации объекта информатизации по требованиям безопасности информации. 18. Тестирование на проникновение в компьютерных системах.	Создан электронный онлайн - курс, размещены материалы к лекциям и лабораторным занятиям.

п/п	Наименование раздела дисциплины	Содержание раздела дисциплины	Реализация раздела дисциплины с помощью онлайн-курса, ЭУМК
Лабораторные занятия			
1	Методы и средства защиты информации на объекте информатизации	Контроль уязвимостей на уровне операционных систем и прикладного ПО	Создан электронный онлайн - курс, размещены материалы к лекциям и лабораторным занятиям.
2	Методы и средства защиты информации на объекте информатизации	Контроль уязвимостей на уровне системы управления базами данных	Создан электронный онлайн - курс, размещены материалы к лекциям и лабораторным занятиям.
3	Методы и средства защиты информации на объекте информатизации	Проверка организации контроля доступа клиентсерверных приложений к объектам баз данных. Разграничение полномочий пользователей с использованием ролей и привилегий	Создан электронный онлайн - курс, размещены материалы к лекциям и лабораторным занятиям.
4	Методы и средства защиты информации на объекте информатизации	Детальный контроль доступа пользователей к базам данных	Создан электронный онлайн - курс, размещены материалы к лекциям и лабораторным занятиям.

п/п	Наименование раздела дисциплины	Содержание раздела дисциплины	Реализация раздела дисциплины с помощью онлайн-курса, ЭУМК
5	Методы и средства защиты информации на объекте информатизации	Мандатный контроль доступа пользователей	Создан электронный онлайн - курс, размещены материалы к лекциям и лабораторным занятиям.
6	Методы и средства защиты информации на объекте информатизации	Контроль аудита действий пользователей средствами разработчика, встроенными средствами СУБД, аудит действий пользователя с привилегией «sysdba»	Создан электронный онлайн - курс, размещены материалы к лекциям и лабораторным занятиям.
7	Методы и средства защиты информации на объекте информатизации	Контроль детального аудита действий пользователей в СУБД	Создан электронный онлайн - курс, размещены материалы к лекциям и лабораторным занятиям.
8	Контроль эффективности защиты информации на объекте информатизации	Контроль восстановления базы данных при разных сценариях потери/повреждения файлов, физического копирования и архивирования данных	Создан электронный онлайн - курс, размещены материалы к лекциям и лабораторным занятиям.
9	Контроль эффективности защиты информации на объекте информатизации	Контроль восстановления базы данных методами логического копирования	Создан электронный онлайн - курс, размещены материалы к лекциям и лабораторным занятиям.

13.2. Темы (разделы) дисциплины и виды занятий

№ п/п	Наименование темы (раздела)	Лекционные занятия	Практические занятия	Лабораторные занятия	Самостоятельная работа	Всего
1	Защита информации на объекте информатизации,основные положения	4			2	6
2	Технические каналы утечки информации	10			4	14
3	Угрозы несанкционированного доступа к информации в компьютерных системах	8			4	12
4	Методы и средства защиты информации на объекте информатизации	8		28	18	54
5	Контроль эффективности защиты информации на объекте информатизации	6		8	8	22
		36	0	36	36	108

14. Методические указания для обучающихся по освоению дисциплины

1) При изучении дисциплины рекомендуется использовать следующие средства**:**

- рекомендуемую основную и дополнительную литературу;
- методические указания и пособия;
- контрольные задания для закрепления теоретического материала;
- электронные версии учебников и методических указаний для выполнения лабораторно - практических работ (при необходимости материалы рассылаются по электронной почте).

2) Для максимального усвоения дисциплины рекомендуется проведение письменного опроса (тестирование, решение задач) студентов по материалам лекций и практических работ. Подборка вопросов для тестирования осуществляется на основе изученного теоретического материала. Такой подход позволяет повысить мотивацию студентов при конспектировании лекционного материала.

3) При проведении лабораторных занятий обеспечивается максимальная степень соответствия с материалом лекционных занятий и осуществляется экспериментальная проверка методов, алгоритмов и технологий обработки информации, излагаемых в рамках лекций.

15. Перечень основной и дополнительной литературы, ресурсов интернет, необходимых для освоения дисциплины

№ п/п	Источник
1	Казарин Олег Викторович. Программно-аппаратные средства защиты информации. Защита программного обеспечения : учебник и практикум для вузов : [для студ. вузов, обучающихся по инженер.-техн. направлениям] / О.В. Казарин, А.С. Забабурин .— Москва : Юрайт, 2018 .— 311, [1] с. : ил., табл. — (Специалист) .— Библиогр. в конце гл. — ISBN 978-5-9916-9043-0.
2	Баранова Елена Константиновна. Информационная безопасность и защита информации : учебное пособие : [для студ., обучающихся по направлению "Прикладная информатика"] / Е.К. Баранова, А.В. Бабаш .— 4-е изд. перераб. и доп. — Москва : РИОР : ИНФРА-М, 2019 .— 334, [1] с. : ил., табл. — (Высшее образование) .— Библиогр.: с. 327-330 .— ISBN 978-5-369-01761-6 .— ISBN 978-5-16-013849-7.
3	Мельников, Владимир Павлович. Информационная безопасность : [учебник для студ. вузов, обучающихся по направлениям подготовки "Конструкторско-технологическое обеспечение машиностроительных производств", "Автоматизация технологических процессов и производств"] / В.П. Мельников, А.И. Куприянов, Т.Ю. Васильева ; под ред. В.П. Мельникова .— 2-е изд., перераб. и доп. — Москва : КноРус, 2018 .— 371 с. : ил., цв. ил., табл. — (Бакалавриат) .— Библиогр.: с. 369-371.

б) дополнительная литература:

№ п/п	Источник
1	Ищейнов Вячеслав Яковлевич. Защита конфиденциальной информации : [учебное пособие для студ. вузов., обуч. по специальности 090103 "Организация и технология защиты информации" и 090104 «Комплексная защита объектов информатизации»] / В.Я. Ищейнов, М.В. Мецатунян .— М. : ФОРУМ, 2009 .— 254 с. : ил. — (Высшее образование) .— Библиогр.: с.249-254 .— ISBN 978-5- 91134-336-1.
2	Хорев Павел Борисович. Методы и средства защиты информации в компьютерных системах: учебное пособие для студ. вузов, обуч. по направлению 230100 (654600) "Информатика и вычислительная техника" / П.Б. Хорев .— М. : ACADEMIA, 2005 .— 254, [1] с. : ил. — (Высшее профессиональное образование. Информатика и вычислительная техника) .— Библиогр.: с. 251- 252 .— ISBN 5-7695-1839-1.
3	Малюк Анатолий Александрович. Информационная безопасность: концептуальные и методологические основы защиты информации : учебное пособие для студ. вузов, обуч. по специальности 075400 - "Комплексная защита объектов информации" / А.А. Малюк .— М. : Горячая линия-Телеком , 2004 .— 280 с. : ил/ .— (Учебное пособие) .— Библиогр.: с. 276-278 .— ISBN 5-93517-197-X.
4	Галицкий, Александр Владимирович. Защита информации в сети - анализ технологий и синтез решений / А.В. Галицкий, С.Д. Рябко, В.Ф. Шаньгин .— М. : ДМК Пресс, 2004 .— 613 с. : ил .— (Администрирование и защита) .— Библиогр.: с.599-608 .— Предм. указ.:с.603-613 .— ISBN 5-94074-244-0.

№ п/п	Источник
5	Варлатая Светлана Климентьевна. Защита и обработка конфиденциальных документов : учебнометодический комплекс / С.К. Варлатая, М.В. Шаханова ; Дальневост. федер. ун-т .— Москва : Проспект, 2015 .— 178, [1] с. : ил., табл. — Библиогр.: с. 177 .— ISBN 978-5-392-19176-5
6	Андрианов В. И. "Шпионские штучки 2", или Как сберечь свои секреты / Под общ. ред. Колесниченко О. В. и др. — СПб. : Полигон, 1997 .— 271 с. — ISBN 5-89173-015-4 : 12.33.

в) информационные электронно-образовательные ресурсы:

№ п/п	Источник
1	Электронный каталог Научной библиотеки Воронежского государственного университета. – (http // www.lib.vsu.ru/).
2	Образовательный портал «Электронный университет ВГУ».– (https://edu.vsu.ru/).
3	ЭБС Лань – Лицензионный договор №3010-14/37-23 от 07.03.2023 (срок предоставления с 12.03.2023 по 11.03.2024) ЭБС «Университетская библиотека online» – Контракт №3010-06/23-22 от 30.12.2022 (срок предоставления с 12.01.2023 по 11.01.2024) ЭБС «Консультант студента» – Лицензионный договор №3010-06/22-22 от 30.12.2022 (с дополнительным соглашение №1 от 09.01.2023) (срок предоставления с 12.01.2023 по 11.01.2024)
4	Меры защиты информации в государственных информационных системах. Методические документы ФСТЭК России. (http://fstec.ru/component/attachments/download/675)
5	Базовая модель угроз безопасности персональных данных при их обработке в информационных системах персональных данных (выписка) (http://fstec.ru/component/attachments/download/289)
6	Методика определения угроз безопасности информации в информационных системах, проект, ФСТЭК России, май 2015 г., Методический документ. (http://fstec.ru/component/attachments/download/812)
7	Методика моделирования угроз безопасности информации. Методические документы ФСТЭК России. (http://fstec.ru/component/attachments/download/2727)
8	Банк данных угроз безопасности информации ФСТЭК России (http://bdu.fstec.ru/)

16. Перечень учебно-методического обеспечения для самостоятельной работы

№ п/п	Источник
1	Грибунин Вадим Геннадьевич. Комплексная система защиты информации на предприятии : [учебное пособие для студ. вузов, обуч. по специальностям "Организация и технология защиты информации", "Комплекс. защита объектов информатизации" направления подготовки "Информ. безопасность"] / В.Г. Грибунин, В.В. Чудовский .— М. : Академия, 2009 .— 411, [1] с. : ил., табл. — (Высшее профессиональное образование. Информационная безопасность) .— Библиогр.: с.403-406.
2	Методика определения угроз безопасности информации в информационных системах, проект, ФСТЭК России, май 2015 г., Методический документ. (http://fstec.ru/component/attachments/download/812).

17. Образовательные технологии, используемые при реализации учебной дисциплины, включая дистанционные образовательные технологии (ДОТ), электронное обучение (ЭО), смешанное обучение):

№ пп	Наименование ПО	Производитель ПО (или торговая марка, Или правообладатель) при наличии	Наименование образовательной программы, в которой используется ПО
	ОС Windows v.7, 8, 10	Microsoft (прим. 1)	Все ОП факультета
	Windows Server v. 2008-2019	Microsoft	Информационные системы и технологии, Информационные системы и сетевые технологии, Информационные системы в телекоммуникациях.
3.	ОС GNU/Linux (CentOS) v.6-8	RedHat, GNU	Все ОП факультета
4.	Платформа электронного обучения LMS-Moodle, основа Образовательного портала «Электронный университет ВГУ»	Moodle Pty Ltd, GNU General Public License	Все ОП факультета
5.	Notepad++	GNU	Все ОП факультета
6.	MySQL Workbench Community	GNU	Все ОП факультета

7.	SecretNet Studio 8 (демоверсия)	ООО Код Безопасности	Компьютерная безопасность, Информационная безопасность
8.	СКЗИ «КриптоПро Рутокен CSP»	Компания КриптоПро (прим. 5)	Компьютерная безопасность, Информационная безопасность

18. Материально-техническое обеспечение дисциплины:

479	Учебная аудитория: компьютер преподавателя i5-8400-2,8ГГц, монитор с ЖК 19", мультимедийный проектор, экран.	394018, г. Воронеж, площадь Университетская, д. 1, корп.1а, ауд. 479
380	Учебная аудитория: компьютер преподавателя i3-3240-3,4ГГц,монитор с ЖК 22", мультимедийный проектор, экран. Система Интернет-видеоконференцсвязи (корп. 1а ауд. 380) Состав системы Интернет-видеоконференцсвязи: ВКС LifeSize Team220 Camera 200 Dual, аудиосистема Defender Mercury 34 SPK-705, интерактивная доска со встроенным проектором "SmartBoard 480iv V25" Лабораторное оборудование по теоретической механике и оптике: машина Атвуда, маятник Максвелла, универсальный маятник, маятник Обербека, крутильный маятник, наклонный маятник, прибор для исследования столкновения шаров, определение скорости полета пули с помощью крутильно-баллистического маятника, изучение законов вращательного движения тел, исследование сложных колебаний, установка для измерения модуля упругости проволоки.	394018, г. Воронеж, площадь Университетская, д. 1, корп.1а, ауд. 380
505	Учебная аудитория: компьютер преподавателя i5-3220-3.3ГГц, монитор с ЖК 17", мультимедийный проектор, экран.	394018, г. Воронеж, площадь Университетская, д. 1, корп.1б, ауд. 505
477	Учебная аудитория: ноутбук HP Pavilion Dv9000-er, мультимедийный проектор, экран.	394018, г. Воронеж, площадь Университетская, д. 1, корп.1а, ауд. 477

292	Учебная аудитория: компьютер преподавателя Pentium-G3420-3,2ГГц, монитор с ЖК 17", мультимедийный проектор, экран. Система для видеоконференций Logitech ConferenceCam Group и ноутбук 15.6" FHD Lenovo V155-15API.	394018, г. Воронеж, площадь Университетская, д. 1, корп.1а, ауд. 292
297	Учебная аудитория: ноутбуки HP EliteBook на базе Intel Core i5-8250U-3.4 ГГц, мониторы ЖК 24" (16 шт.), мультимедийный проектор, экран.	394018, г. Воронеж, площадь Университетская, д. 1, корп.1а, ауд. 297
290	Учебная аудитория: персональные компьютеры на базе i7-7800x-4ГГц, мониторы ЖК 27" (12 шт.), мультимедийный проектор, экран. Лабораторное оборудование искусственного интеллекта: рабочие места - персональные компьютеры на базе i7-7800x-4ГГц, мониторы ЖК 27" (12 шт.); модули АО НПЦ "ЭЛВИС" : процессорный Салют-ЭЛ24ПМ2 (9 шт.), отладочный Салют-ЭЛ24ОМ1 (9 шт.), эмулятор MC-USB-JTAG (9 шт.). Лабораторное оборудование электроники, электротехники и схемотехники: рабочие места - персональные компьютеры на базе i7-7800x-4ГГц, мониторы ЖК 27" (12 шт.); стенд для практических занятий по электрическим цепям (KL-100); стенд для изучения аналоговых электрических схем (KL-200); стенд для изучения цифровых схем (KL-300).	394018, г. Воронеж, площадь Университетская, д. 1, корп.1а, ауд. 290
291	Учебная аудитория: персональные компьютеры на базе i3-3220-3,3ГГц, мониторы ЖК 19" (16 шт.), мультимедийный проектор, экран.	394018, г. Воронеж, площадь Университетская, д. 1, корп.1б, ауд. 291
293	Учебная аудитория: персональные компьютеры на базе Core i7-11700K-3.6 ГГц, мониторы ЖК 24" (15 шт.), мультимедийный проектор, экран. Лабораторное оборудование компьютерной графики видеоадаптеры GeForce RTX 3070.	394018, г. Воронеж, площадь Университетская, д. 1, корп.1б, ауд. 293

295	Учебная аудитория: персональные компьютеры на базе i3-9100-3,6ГГц, мониторы ЖК 24" (14 шт.), мультимедийный проектор, экран. Лабораторное оборудование информационной безопасности операционных систем и программных средств защиты информации от несанкционированного доступа: рабочие места - персональные компьютеры на базе Intel i3-9100-3,6ГГц, , мониторы ЖК 24" (14 шт.); учебный стенд «Программные средства защиты информации от несанкционированного доступа».	394018, г. Воронеж, площадь Университетская, д. 1, корп.1б, ауд. 295
305	Учебная аудитория: ноутбук HP Pavilion Dv9000-er, мультимедийный проектор, экран.	394018, г. Воронеж, площадь Университетская, д. 1, корп.1б, ауд. 305
307	Учебная аудитория: ноутбук HP Pavilion Dv9000-er, мультимедийный проектор, экран.	394018, г. Воронеж, площадь Университетская, д. 1, корп.1б, ауд. 307

303	Учебная аудитория: персональные компьютеры на базе i3-8100-3,9ГГц, мониторы ЖК 24" (13 шт.), мультимедийный проектор, экран. Лабораторное оборудование программно-аппаратных средств обеспечения информационной безопасности: персональные компьютеры на базе Intel i3-8100 3.60ГГц, мониторы ЖК 19" (10 шт.), стойка (коммуникационный шкаф), управляемый коммутатор HP Procurve 2524, аппаратный межсетевой экран D-Link DFL-260E, аппаратный межсетевой экран CISCO ASA-5505. лабораторная виртуальная сеть на базе Linux-KVM/LibVirt, взаимодействующая с сетевыми экранами. USB-считыватели смарт-карт ACR1281U-C1 и ACR38U-NEO, смарт-карты ACOS3 72K+MIFARE, карты памяти SLE4428/SLE5528. Учебно-методический комплекс "Программно-аппаратная защита сетей с защитой от НСД" ОАО "ИнфоТеКС". Лабораторное оборудование технической защиты информации, состав ST03ЗР "Пиранья" - многофункциональный поисковый прибор, ST03.DA - дифференциальный низкочастотный усилитель, ST03.TEST - контрольное устройство; комплекс виброакустической защиты "Соната": Соната-ИПЗ, Соната-СА-65М, Соната-СВ-45М; генератор-виброизлучатель (5 октав) "ГШ-1000У"; генератор шума для защиты объектов вычислительной техники 1, 2 и 3 категорий от утечки информации; система автоматизированная оценки защищенности технических средств от утечки информации по каналу побочных электромагнитных излучений и наводок <Сигурд>. Программно-аппаратный комплекс для мониторинга радиообстановки в диапазоне 9 кГц - 21 ГГц «Кассандра К21». Комплекс оценки эффективности защиты речевой информации от утечки по акустическому и виброакустическому каналам, 20 – 12500 Гц.	394018, г. Воронеж, площадь Университетская, д. 1, корп.1б, ауд. 303
314	Учебная аудитория: персональные компьютеры на базе i3-7100-3,6ГГц, мониторы ЖК 19" (16 шт.), мультимедийный проектор, экран.	394018, г. Воронеж, площадь Университетская, д. 1, корп.1б, ауд. 314
316	Учебная аудитория: персональные компьютеры на базе i3-9100-3,6ГГц, мониторы ЖК 19" (30 шт.), мультимедийный проектор, экран.	394018, г. Воронеж, площадь Университетская, д. 1, корп.1б, ауд. 316

381	Учебная аудитория: компьютер преподавателя i3-540-3ГГц, мультимедийный проектор, экран.	394018, г. Воронеж, площадь Университетская, д. 1, корп.1а, ауд. 381
382	Учебная аудитория: персональные компьютеры на базе i5-9600KF-3,7ГГц, мониторы ЖК 24" (16 шт.), ТВ панель-флипчарт.	394018, г. Воронеж, площадь Университетская, д. 1, корп.1а, ауд. 382
383	Учебная аудитория: персональные компьютеры на базе i7-9700F-3ГГц, мониторы ЖК 27" (16 шт.), мультимедийный проектор, экран. Лабораторное оборудование мобильных приложений и игр: рабочие места - персональные компьютеры на базе Intel i7-9700F, видеоадаптеры nVidia GeForce RTX2070, мониторы ЖК 27" (16 шт.); Системы виртуальной реальности HTC Vive Cosmos (2шт.); Беспроводный маршрутизатор TP-Link Archer C7. Лабораторное оборудование безопасности компьютерных сетей: рабочие места - персональные компьютеры HP-3500-PRO на базе Intel i3-2120, мониторы ЖК 22" (16 шт.), стойка (коммуникационный шкаф), управляемый коммутатор CISCO Catalyst 2950, маршрутизатор CISCO 2811-ISR, аппаратный межсетевой экран CISCO серии ASA-5500. лабораторная виртуальная сеть на базе Linux-KVM/LibVirt, взаимодействующая с перечисленным сетевым оборудованием. Программный анализатор сетевого трафика WireShark. Программный симулятор Packet Tracer, для создания виртуальных стендов, включающих коммутаторы 2 и 3 уровней, маршрутизаторы, сетевые экраны и СОВ. Учебно-методический комплекс "Безопасность компьютерных сетей" ОАО "ИнфоТеКС".	394018, г. Воронеж, площадь Университетская, д. 1, корп.1а, ауд. 383
384	Учебная аудитория: персональные компьютеры на базе i3-2120-3,3ГГц, мониторы ЖК 22" (16 шт.), мультимедийный проектор, экран.	394018, г. Воронеж, площадь Университетская, д. 1, корп.1а, ауд. 384
385	Учебная аудитория: персональные компьютеры на базе i3-2120-3,3ГГц, мониторы ЖК 19" (16 шт.), мультимедийный проектор, экран.	394018, г. Воронеж, площадь Университетская, д. 1, корп.1а, ауд. 385

387	Учебная аудитория: компьютер преподавателя Core2Duo-E7600-3ГГц, монитор с ЖК 22", мультимедийный проектор, экран. Персональные компьютеры студентов на базе i5-10400-2,9ГГц, мониторы ЖК 27" (11 шт.).	394018, г. Воронеж, площадь Университетская, д. 1, корп.1а, ауд. 387
308	Учебная аудитория: видеомагнитофоны Philips, Samsung, аудиомагнитофоны Panasonic, Sony.	394018, г. Воронеж, площадь Университетская, д. 1, корп.1б, ауд. 308
309	Учебная аудитория: видеомагнитофоны Philips, Samsung, аудиомагнитофоны Panasonic, Sony.	394018, г. Воронеж, площадь Университетская, д. 1, корп.1б, ауд. 309
301	Учебная аудитория: персональные компьютеры на базе i3-2120-3,3ГГц, мониторы ЖК 17" (15 шт.), мультимедийный проектор, экран. Лабораторное оборудование суперкомпьютерного центра: кластер с пиковой производительностью 40 Tflops. Состав кластера: 10 узлов, каждый имеет два 12-ядерных процессора Intel Xeon E5-2680V3, 128 Гбайт ОЗУ, SSD 256 Гбайт. 7 узлов из 10 содержат по 2 ускорителя Intel Xeon Phi 7120, 3 узла - 2 ускорителя Tesla K80M. Все узлы объединены высокоскоростной сетью InfiniBand 56 Gbps; управляющий узел кластера (также сервером для хранения файлов): два 6-ядерных процессора, 64 Гбайт оперативной памяти и дисковую подсистему объемом 14 ТБайт; сервер для занятий по параллельному программированию: Intel X5650@2.67GHz 12 ядер 24 потоков, ОЗУ 36ГБ, дисковая подсистема объемом 300ГБ.	394018, г. Воронеж, площадь Университетская, д. 1, корп.1б, ауд. 301
190а	Лабораторное оборудование медицинской кибернетики: рабочие места - персональные компьютеры на базе Intel i3-2120, мониторы ЖК 19" (3 шт.); электроэнцефалограф Нейрон-спектр-4 (2 шт.); кардиограф Полиспектр-12 (1 шт.); оптические микросокопы Р-1 (2 шт.); 3D-принтер (1 шт.); паяльные станции (2 шт.).	394018, г. Воронеж, площадь Университетская, д. 1, корп.1б, ауд. 190а

403	Учебная аудитория: персональные компьютеры на базе i3-2320-3,3ГГц, мониторы ЖК 22" (7 шт.), мультимедийный проектор, экран. Лабораторное оборудование физической лаборатории с комплектом оборудования по квантовой физике: Установка для изучения космических лучей (ФПК-01); установка для определения резонансного потенциала методом Франка и Герца (ФПК-02); установка для определения длины свободного пробега частиц в воздухе (ФПК-03); установка для изучения энергетического спектра электронов (ФПК-05); установка для изучения p-n перехода (ФПК-06); установка для изучения температурной зависимости электропроводности металлов и полупроводников (ФПК-07); установка для изучения эффекта Холла в полупроводниках (ФПК-08); установка для изучения спектра атома водорода (ФПК-09); установка для изучения внешнего фотоэффекта (ФПК-10); установка для изучения абсолютно черного тела (ФПК-11); установка для изучения работы сцинтилляционного счетчика (ФПК-12); установка для изучения и анализа свойств материалов с помощью сцинтилляционного счетчика (ФПК-13).	394018, г. Воронеж, площадь Университетская, д. 1, корп.1б, ауд. 403
420	Лабораторное оборудование по электротехники и электроники: лабораторные стенды: полупроводниковые диоды, фотодиод, биполярный транзистор, полевой транзистор, операционный усилитель, многокаскадовый RC-усилитель, амплитудный модулятор и демодулятор, LC-генератор с индуктивной обратной связью, кварцевый генератор, RC-генератор с фазосдвигающей цепью, мультивибратор, триггер на биполярном транзисторе, основные схемы выпрямителей, универсальные логические элементы ТТЛ, регистр сдвига, счетчик	394018, г. Воронеж, площадь Университетская, д. 1, корп.1б, ауд. 420
425	Лабораторное оборудование сетей и систем передачи информации: стойка (коммуникационный шкаф), 3 коммутатора CISCO WS-C2960-24TT-L, 3 маршрутизатора CISCO 2801, 2 WiFi-маршрутизатора Linksys WRT54G.	394018, г. Воронеж, площадь Университетская, д. 1, корп.1, ауд. 425

19. Оценочные средства для проведения текущей и промежуточной аттестаций

Порядок оценки освоения обучающимися учебного материала определяется содержанием следующих разделов дисциплины:

№ п/п	Разделы дисциплины (модули)	Код компетенции	Код индикатора	Оценочные средства для текущей аттестации
1	Защита информации на объекте информатизации,основные положения. Угрозы несанкционированного доступа к информации в компьютерных системах	ОПК-8	ОПК-8.1	Устный опрос
2	Угрозы несанкционированного доступа к информации в компьютерных системах	ОПК-8	ОПК-8.2	Устный опрос
3	Угрозы несанкционированного доступа к информации в компьютерных системах	ОПК-8	ОПК-8.3	Устный опрос
4	Угрозы несанкционированного доступа к информации в компьютерных системах Контроль эффективности защиты информации на объекте информатизации	ОПК-8	ОПК-8.4	Устный опрос Лабораторные работы
5	Угрозы несанкционированного доступа к информации в компьютерных системах	ОПК-8	ОПК-8.5	Устный опрос
6	Угрозы несанкционированного доступа к информации в компьютерных системах Контроль эффективности защиты информации на объекте информатизации.	ОПК-8	ОПК-8.6	Устный опрос Лабораторные работы
7	Защита информации на объекте информатизации,основные положения.	ОПК-12	ОПК-12.1	Устный опрос
8	Защита информации на объекте информатизации,основные положения. Угрозы несанкционированного доступа к информации в компьютерных системах Контроль эффективности защиты информации на объекте информатизации.	ОПК-12	ОПК-12.2	Устный опрос
9	Угрозы несанкционированного доступа к информации в компьютерных системах	ОПК-12	ОПК-12.3	Устный опрос

№ п/п	Разделы дисциплины (модули)	Код компетенции	Код индикатора	Оценочные средства для текущей аттестации
10	Угрозы несанкционированного доступа к информации в компьютерных системах	ОПК-12	ОПК-12.4	Устный опрос
11	Технические каналы утечки информации Методы и средства защиты информации на объекте информатизации	ОПК-12	ОПК-12.5	Устный опрос Лабораторные работы
12	Защита информации на объекте информатизации,основные положения. Контроль эффективности защиты информации на объекте информатизации	ОПК-12	ОПК-12.6	Устный опрос Лабораторные работы
13	Контроль эффективности защиты информации на объекте информатизации	ОПК-12	ОПК-12.7	Устный опрос Лабораторные работы
14	Защита информации на объекте информатизации,основные положения. Контроль эффективности защиты информации на объекте информатизации	ОПК-12	ОПК-12.8	Устный опрос Лабораторные работы
15	Контроль эффективности защиты информации на объекте информатизации	ОПК-12	ОПК-12.9	Устный опрос Лабораторные работы

Промежуточная аттестация

Форма контроля - Экзамен

Оценочные средства для промежуточной аттестации

Примерный перечень применяемых оценочных средств

№ п/п	Наименование оценочного средства	Представление оценочного средства в фонде	Критерии оценки
1	2	3	4
1	Устный опрос	Вопросы по темам/разделам дисциплины	Шкала оценивания соответствует приведенной в разделе 20.2

2	Контрольная работа по разделам дисциплины	Теоретические вопросы по темам/разделам дисциплины	Шкала оценивания соответствует приведенной в разделе 20.2
3	Лабораторная работа	Содержит 5 лабораторных заданий, предусматривающих разработку и тестирование криптографических и стеганографических алгоритмов	При успешно выполнении работы осуществляется допуск к контрольной работе, в противном случае обучающийся не допускается к контрольной работе.
4	КИМ промежуточной аттестации	Каждый контрольно-измерительный материал для проведения промежуточной аттестации включает 2 вопроса для контроля знаний, умений и владений в рамках оценки уровня сформированности компетенции.	Шкалы оценивания приведены в разделе 20.2

20 Типовые оценочные средства и методические материалы, определяющие процедуры оценивания

20.1 Текущий контроль успеваемости

Контроль успеваемости по дисциплине осуществляется с помощью следующих оценочных средств:

Пример лабораторной работы

Лабораторная работа №1

«Контроль уязвимостей на уровне операционных систем и прикладного ПО»

Цель работы: Получение практических навыков анализа работы сканера безопасности на уровне закрытия уязвимостей.

Вариант задания. Проверка доступности узлов сети. Формирование плана проверок узлов сети. Проведение проверок согласно сформированному плану. Просмотр результатов работы проверок и формирование отчетов.

Описание технологии проведения

Оценка знаний, умений и навыков, характеризующая этапы формирования компетенций в рамках изучения дисциплины осуществляется в ходе текущей и промежуточной аттестаций.

Текущая аттестация проводится в соответствии с Положением о текущей аттестации обучающихся по программам высшего образования Воронежского государственного университета. Текущая аттестация проводится в формах устного опроса (индивидуальный опрос, фронтальная беседа) и письменных работ (контрольные, лабораторные работы). При оценивании могут использоваться количественные или качественные шкалы оценок.

Требования к выполнению заданий (или шкалы и критерии оценивания)

При оценивании используется количественная шкала. Критерии оценивания приведены выше в

таблице раздела 20.2.

20.2 Промежуточная аттестация

Промежуточная аттестация по дисциплине осуществляется с помощью следующих оценочных средств:

Примерный перечень вопросов к экзамену

№	Содержание
1	Средства и меры защиты конфиденциальности, целостности, доступности информации на объекте информатизации.
2	Лицензирование деятельности в области защиты информации.
3	Технические каналы утечки информации на объектах информатизации.
4	*Организация работ по защите конфиденциальной информации на объекте информатизации.*
5	*Требования и рекомендации по защите речевой конфиденциальной информации.*
6	*Угрозы утечки информации с использованием линий связи и защита от них.*
7	*Основные требования и рекомендации по защите информации, циркулирующей в защищаемых помещениях.*
8	*Материально-вещественные каналы утечки информации.*
9	*Методы и средства несанкционированного получения информации по техническим каналам.*
10	*Угрозы несанкционированного доступа к информации в компьютерных системах.*
11	*Модель угроз безопасности информации.*
12	Методика определения угроз безопасности информации в информационных системах.
13	*Банк данных угроз безопасности информации.*
14	*Модель нарушителя безопасности информации.*
15	*Закладные программно-технические средства и возможные способы защиты от них.*
16	Виды ущерба безопасности информации и методы его оценки. Технико-экономическое обоснование комплекса мер по обеспечению информационной безопасности.
17	*Методы и средства защиты информации на объекте информатизации.*
18	*Типовые аппаратные средства защиты информации на объектах информатизации.*

19	Типовые программные и программно-аппаратные средства защиты информации на объектах информатизации.
20	Требования и меры безопасности информации при использовании криптографических средств защиты.
21	Комплексное обеспечение защиты информации на объекте информатизации.
22	Контроль эффективности защиты информации на объекте информатизации.
23	Аттестации объекта информатизации по требованиям безопасности информации.
24	Тестирование на проникновение в компьютерных системах.
25	Уязвимости в информационных системах и основные методы защиты.

Пример контрольно-измерительного материала

УТВЕРЖДАЮ

Заведующий кафедрой технологий обработки и защиты информации

_____ А.А. Сирота

__.__.2023

Направление подготовки / специальность 10.03.01 Информационная безопасность

Дисциплина Б1.О.45 Комплексное обеспечение защиты информации объекта информатизации

Форма обучения Очное

Вид контроля Экзамен

Вид аттестации Промежуточная

Контрольно-измерительный материал № 1

1. Средства и меры защиты конфиденциальности, целостности, доступности информации на объекте информатизации.
2. Тестирование на проникновение в компьютерных системах.

Преподаватель _____ А.Ю. Иванков

Описание технологии проведения

Для оценивания результатов обучения на зачете используются следующие содержательные показатели (формулируется с учетом конкретных требований дисциплины):

1. знание теоретических основ учебного материала, основных определений, понятий и используемой терминологии;

2. умение проводить обоснование и представление основных теоретических и практических результатов (алгоритмов, методик) с использованием математических выкладок, блок-схем, структурных схем и стандартных описаний к ним;

3. умение обосновывать свои суждения и профессиональную позицию по излагаемому вопросу;

4. владение навыками программирования и исследования криптографических алгоритмов обработки информации в рамках выполняемых лабораторных заданий;

Различные комбинации перечисленных показателей определяют критерии оценивания результатов обучения (сформированности компетенций) на государственном экзамене:

- пороговый (базовый) уровень сформированности компетенций.

Для оценивания результатов обучения на государственном экзамене используется 4-балльная шкала: «отлично», «хорошо», «удовлетворительно», «неудовлетворительно». Для оценивания результатов обучения на зачете используется – зачтено, не зачтено по результатам тестирования.

Требования к выполнению заданий, шкалы и критерии оценивания

Критерии оценивания компетенций и шкала оценок (экзамен)

Критерии оценивания компетенций	Уровень сформированности компетенций	Шкала оценок
Обучающийся демонстрирует полное соответствие знаний, умений, навыков по приведенным критериям свободно оперирует понятийным аппаратом и приобретенными знаниями, умениями, применяет их при решении практических задач. Успешно выполнены лабораторные работы в соответствии с установленным перечнем.	Повышенный уровень	Отлично
Ответ на контрольно-измерительный материал не полностью соответствует одному из перечисленных выше показателей, но обучающийся дает правильные ответы на дополнительные вопросы. При этом обучающийся демонстрирует соответствие знаний, умений, навыков приведенным в таблицах показателям, но допускает незначительные ошибки, неточности, испытывает затруднения при решении практических задач. Успешно выполнены лабораторные работы в соответствии с установленным перечнем.	Базовый уровень	Хорошо
Обучающийся демонстрирует неполное соответствие знаний, умений, навыков приведенным в таблицах показателям, допускает значительные ошибки при решении практических задач. При этом ответ на контрольно-измерительный материал не соответствует любым двум из перечисленных показателей, обучающийся дает неполные ответы на дополнительные вопросы. Успешно выполнены лабораторные работы в соответствии с установленным перечнем.	Пороговый уровень	Удовлетворительно
Ответ на контрольно-измерительный материал не соответствует любым трем из перечисленных показателей. Обучающийся демонстрирует отрывочные, фрагментарные знания, допускает грубые ошибки. Не выполнены лабораторные работы в соответствии с установленным перечнем.	–	Неудовлетворительно

20.3 Фонд оценочных средств для проверки остаточных знаний (может быть использован для проведения экзамена в дистанционном режиме)

Компетенция ОПК-8

Вопросы с выбором ответа

1. Какие из перечисленных информационных потоков относятся к побочным информационным процессам взаимодействии объекта информатизации с внешней средой?

а) электромагнитные излучения технических средств обработки и передачи информации, при этом сигналы, несущие информацию, можно принять специальной аппаратурой;

б) побочные наводки в результате электромагнитных излучений технических средств или виброакустических эффектов на окружающую передающую среду, из которой можно извлечь информацию;

в) выход информации за пределы объекта за счёт непродуманных действий служащих (некорректная реклама, бесконтрольное уничтожение отходов - носителей информации и т.д.);

г) возможность получения информации от служащих объекта как носителей информации (человеческий фактор) и другие проявления;

д) всё перечисленные информационные потоки.

2. Какие из перечисленных информационных потоков относятся к штатным каналам информационного взаимодействия объекта информатизации с внешней средой?

а) все виды электрической связи (телефонная, мобильная и т.д.);

б) штатные документальные потоки, связанные с документальным информационным взаимодействием, управлением, отчетностью и т.д.;

в) побочные наводки в результате электромагнитных излучений технических средств или виброакустических эффектов на окружающую передающую среду, из которой можно извлечь информацию;

г) возможность получения информации от служащих объекта как носителей информации (человеческий фактор) и другие проявления;

д) всё перечисленные информационные потоки.

3. Сущность принципа комплексности защиты информации состоит в:

а) оптимальном использование различных методов, мер и средств защиты информации для нейтрализации угроз информации и поддержания заданного уровня защищенности информации, интеграции этих средств в единую технологически связанную и управляемую систему;

б) обеспечении непрерывного целенаправленного процесса, предполагающего принятие соответствующих мер на всех этапах жизненного цикла автоматизированной системы, начиная с самых ранних стадий проектирования, а не только на этапе ее эксплуатации;

в) обеспечении оптимального уровня защиты, при котором затраты, риск и размер возможного ущерба были бы приемлемыми;

г) обеспечении возможности варьирования уровнем защищенности и средствами защиты.

4. Сущность принципа разумной достаточности защиты информации состоит в:

а) оптимальном использование различных методов, мер и средств защиты информации для нейтрализации угроз информации и поддержания заданного уровня защищенности информации, интеграции этих средств в единую технологически связанную и управляемую систему;

б) обеспечении непрерывного целенаправленного процесса, предполагающего принятие соответствующих мер на всех этапах жизненного цикла автоматизированной системы, начиная с самых ранних стадий проектирования, а не только на этапе ее эксплуатации;

в) обеспечении оптимального уровня защиты, при котором затраты, риск и размер возможного ущерба были бы приемлемыми;

г) обеспечении возможности варьирования уровнем защищенности и средствами защиты.

5. Какая из перечисленных подсистем защиты информации объекта информатизации (ОИ) относится к группе защиты при внешнем информационном проявлении ОИ?

а) подсистема предотвращения скрытого внедрения в программные и технические средства программно-технического комплекса и телекоммуникационных сетей;

б) подсистема нейтрализации побочного информационного проявления ОИ;

в) подсистема предотвращения компьютерных атак в автоматизированных системах и ликвидации их последствий;

г) подсистема обеспечения целостности и сохранности информационных ресурсов;

д) подсистема защиты информации в каналах передачи данных на ОИ.

6. Какое из перечисленных определений соответствует понятию объект информатизации?

а) совокупность информационных ресурсов, средств и систем обработки информации, а также средств и систем жизнеобеспечения объекта информатизации, необходимых для установки и эксплуатации средств и систем обработки информации, реализации информационных технологий;

б) совокупность информационных ресурсов, средств и систем обработки информации, используемых в соответствии с заданной информационной технологией, а также средств их обеспечения, помещений или объектов (зданий, сооружений, технических средств), в которых эти средства и системы установлены, или помещений и объектов, предназначенных для ведения конфиденциальных переговоров;

в) общесистемный структурный компонент комплексной системы защиты информации, предназначенный для постоянного поддержания заданного уровня информационной безопасности в автоматизированной системы и на объект информатизации и обеспечивающий эффективную реализацию процессов управления, скоординированных и взаимоувязанных с управлением информационными технологиями.

7. Государственная структура, осуществляющая регулирование в области использования криптографических средств и систем, расположенных на территории РФ:

а) Межведомственная комиссия по защите государственной тайны;

б) Федеральная служба по техническому и экспортному контролю;

в) Федеральная служба безопасности.

8. Какому понятию соответствует следующее определение: преднамеренно или случайно оставленные в программно-технической среде скрытые внедрения, позволяющие изменить политику информационной безопасности, а также выполнять недекларированные действия?

а) аппаратные закладки;

б) программные закладки;

в) вредоносные программы.

9. Что является особенностью стелс-вирусов?

а) поражают программу-загрузчик операционной системы, размещаясь либо в секторе BOOT2 при загрузке системы с внешнего носителя, либо в секторе BOOT1 при загрузке с винчестера;

б) оставляют в оперативной памяти специальные модули, которые перехватывают обращение программ к дисковой подсистеме компьютера и подменяют читаемые данные при обращении к зараженному файлу или системной области диска, имитируя отсутствие вируса;

в) реализуются средствами языков программирования макросов, используемых для автоматизации выполнения повторяющихся действий в табличных редакторах, текстовых процессорах, системах проектирования и т.п.

10. Какие последствия могут иметь место в результате несанкционированного доступа к информации?

а) реализация угрозы конфиденциальности информации;

б) реализация угрозы целостности информации;

в) раскрытие параметров системы;

г) всё перечисленное.

11. Какие способы несанкционированного доступа возможны, если источником конфиденциальной информации являются технические средства?

а) перехват, инициативное сотрудничество, уничтожение

б) копирование, модификация, незаконное подключение;

в) фотографирование, подслушивание переговоров, сбор и аналитическая обработка.

12. К какой категории методов защиты от несанкционированного доступа относятся механизмы разработки и совершенствования нормативной базы, регулирующей вопросы защиты информации?

а) организационные (в т. ч. административные);

б) технологические (или инженерно-технические);

в) правовые;

г) финансовые.

13. Примером динамических признаков биометрической аутентификации является:

а) дактилоскопия (отпечатки пальцев);

б) почерк (в т. ч. клавиатурный почерк);

в) карта памяти с микрочипом;

14. Если для слабой хеш-функции h(x) имеет место сложность в подборе пары таких сообщений x, y, что h(x) = h(y), то такая функция является:

а) сильной;

б) сложной;

в) стойкой.

15. Какой из алгоритмов шифрования использует сложность операции разложения произведения двух простых чисел на сомножители:

а) DES;

б) RSA;

в) ГОСТ 34.12-2018.

16. Каким документом регламентируется правовая сторона разработки и использования средств криптографической защиты информации?

а) Указ Президента Российской Федерации от 03.04.95 № 334 с учетом принятых ранее законодательных и нормативных актов РФ;

б) Система сертификации средств криптографической защиты информации РОСС.RU.0001.030001;

в) Положение о сертификации средств защиты информации по требованиям безопасности информации.

17. Какими основными свойствами характеризуется информация с точки зрения информационной безопасности?

а) целостность;

б) полнота;

в) доступность;

г) адекватность;

д) конфиденциальность;

е) секретность.

18. Какое определение характеризует свойство целостности информации?

а) состояние информации, при котором доступ к ней осуществляют только субъекты, имеющие на него право;

б) состояние информации, при котором отсутствует любое ее изменение либо изменение осуществляется только преднамеренно субъектами, имеющими на него право;

в) состояние информации, при котором субъекты, имеющие права доступа, могут реализовать их беспрепятственно.

19. Что такое CWE?

а) общий перечень ошибок, приводящих к уязвимостям;

б) стандартизированный перечень общеизвестных уязвимостей информационной безопасности;

в) открытый отраслевой стандарт, используемый для оценки уязвимостей.

20. Что такое CVSS?

а) общий перечень ошибок, приводящих к уязвимостям;

б) стандартизированный перечень общеизвестных уязвимостей информационной безопасности;

в) открытый отраслевой стандарт, используемый для оценки уязвимостей.

Вопросы с коротким ответом

1. Какое понятие характеризуется следующим определением: совокупность информационных ресурсов, средств и систем обработки информации, используемых в соответствии с заданной информационной технологией, а также средств их обеспечения, помещений или объектов (зданий, сооружений, технических средств), в которых эти средства и системы установлены, или помещений и объектов, предназначенных для ведения конфиденциальных переговоров?

2. Какая подсистема КСЗИ характеризуется следующим определением: совокупность мер и средств реализации функциональных задач защиты информации, однородных по своей природе или относящихся к определенной сфере обеспечения условий для реализации функциональных задач защиты информации?

3. Какая подсистема КСЗИ включает в себя служебные базы и массивы данных автоматизированной, обеспечивает информационную поддержку реализации функциональных задач защиты информации и принятие решений при управлении информационной безопасностью, содержит все данные для принятия решений при реализации управления, как в технологических процессах, так и на макроуровне?

4. Какое понятие определяется следующим образом: доступ к информации, нарушающий правила разграничения доступа с использованием штатных средств, предоставляемых средствами вычислительной техники или автоматизированными системами?

5. Запишите вектор уязвимости в формате CVSS версии 3.1 с базовыми метрическими значениями Attack Vector: Network, Attack Complexity: Low, Privileges Required: High, User Interaction: None, Scope: Unchanged, Confidentiality: High, Integrity: High, Availability: Low и отсутствующими временными и контекстными метриками.

Вопросы с развернутым ответом

1. Нарисуйте структурную схему информационного представления объекта информатизации при взаимодействии с внешней средой.

Критерии оценивания	Шкала оценок
В схеме присутствуют блоки объекта информатизации (объект защиты), включающего внутреннюю информационную сферу, и внешней среды, включающей объекты штатного информационного взаимодействия (другие объекты информатизации) и средства, реализующие побочное информационное проявление. Обозначены штатные каналы передачи информации (системы передачи данных и связи, документооборот и т.п.) и побочные информационные потоки (процессы).	3 балла

В схеме присутствуют блоки объекта информатизации (объект защиты) и внешней среды, включающей объекты штатного информационного взаимодействия факторы побочного информационного проявления. Обозначены штатные каналы передачи информации (системы передачи данных и связи, документооборот и т.п.) и побочные информационные потоки (процессы). Допускаются незначительные неточности.	2 балла
В схеме присутствуют блоки объекта информатизации и внешней среды, обозначены элементы штатного и побочного информационного взаимодействия, обозначены соответствующие каналы передачи информации. Ответ не содержит грубых ошибок.	1 балл
Отсутствуют элементы штатного и побочного информационного взаимодействия объекта информатизации и внешней среды. Присутствуют грубые ошибки или неточности.	0 баллов

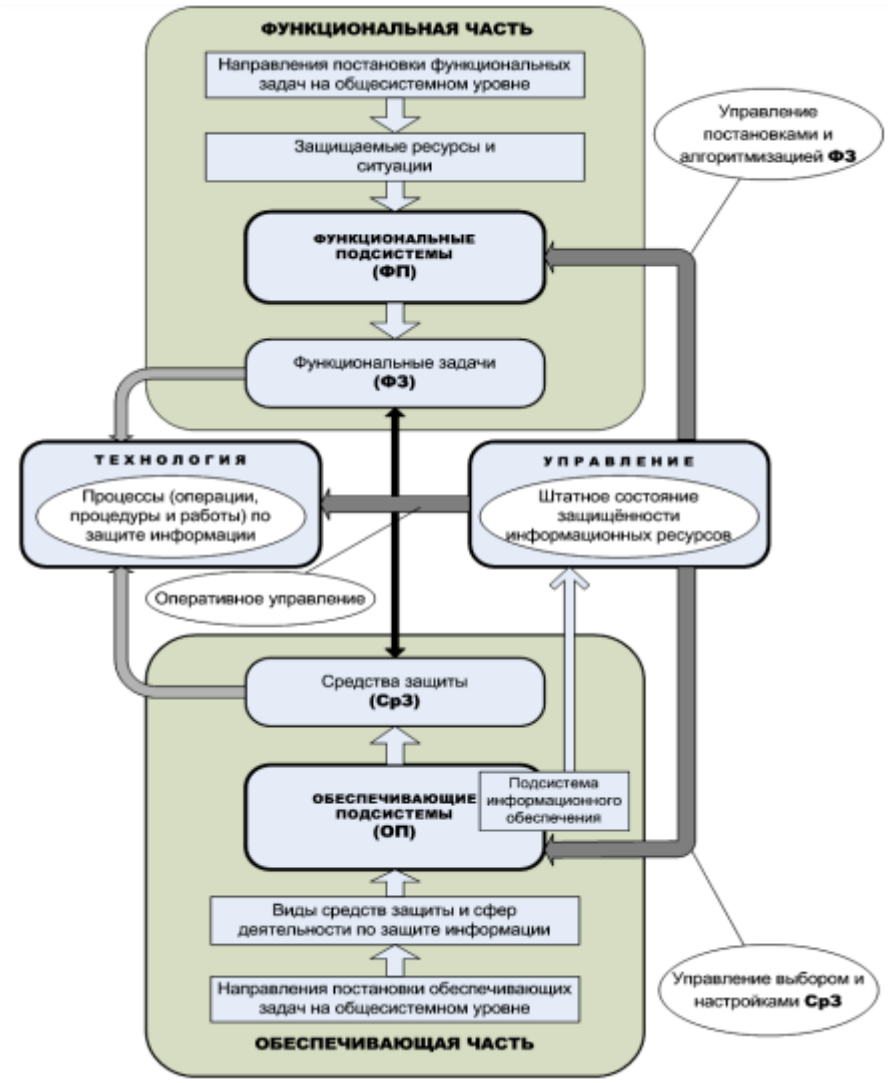
Примерное решение:

2. Нарисуйте структурную схему построения комплексной системы защиты на объекте информатизации.

Критерии оценивания	Шкала оценок

В схеме присутствуют блоки функциональной и обеспечивающих частей, связанные друг с другом и с компонентом технологии, а также компонент управления связывающий их все. В блоках функциональной и обеспечивающей частей отражены элементы синтеза функциональной и обеспечивающей подсистем защиты информации. Обозначены связи между структурными элементами.	3 балла
В схеме присутствуют блоки функциональной и обеспечивающих частей, связанные друг с другом и с компонентом технологии, а также компонент управления связывающий их все. В блоках функциональной и обеспечивающей частей присутствуют элементы функциональной и обеспечивающей подсистем защиты информации. Показаны связи между структурными элементами. Допускаются незначительные неточности.	2 балла
В схеме присутствуют все структурные компоненты. В блоках функциональной и обеспечивающей частей присутствуют элементы функциональной и обеспечивающей подсистем защиты информации. Показаны основные связи между структурными компонентами, без указания направления информационного взаимодействия. Ответ не содержит грубых ошибок.	1 балл
Отсутствуют структурные компоненты или большинство связей. Присутствуют грубые ошибки или неточности.	0 баллов

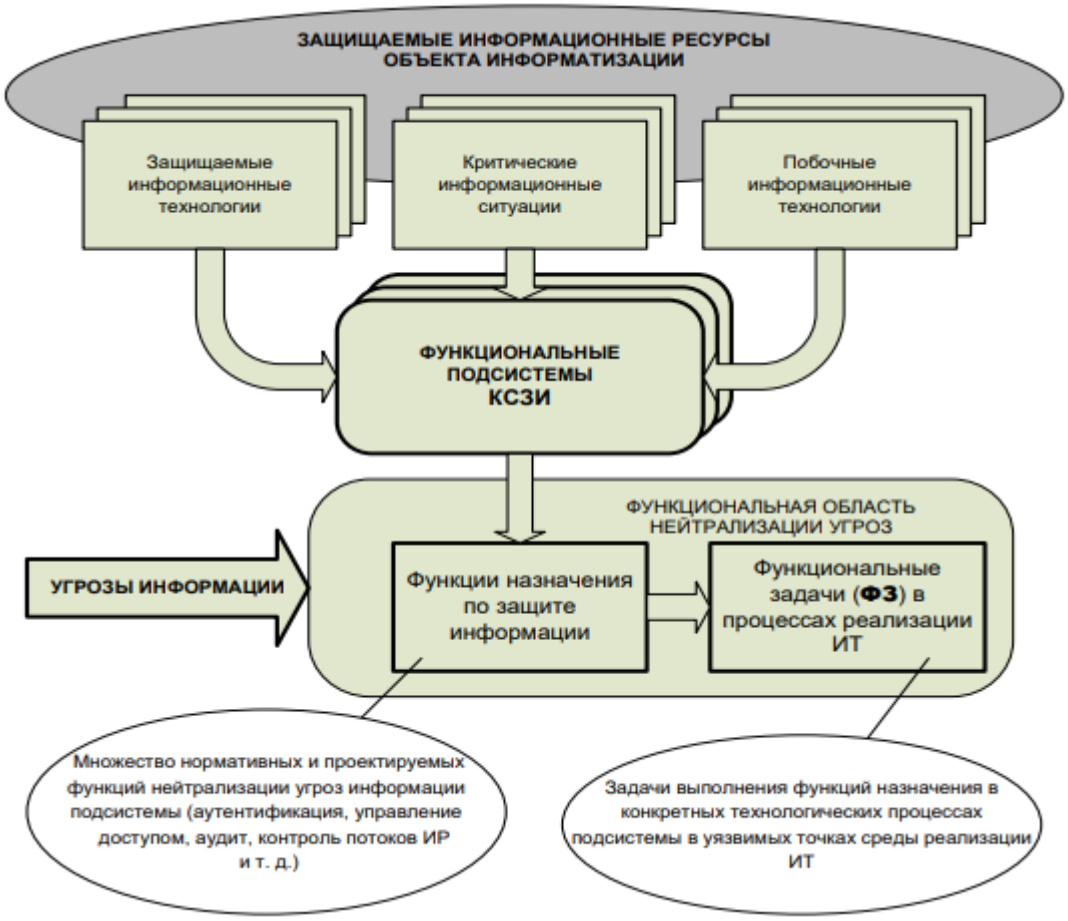
Примерное решение:



3. Нарисуйте схему формирования функциональных подсистем комплексной системы защиты на объекте информатизации.

Критерии оценивания	Шкала оценок
В схеме обозначены основные защищаемые ресурсы, описаны элементы функциональной области нейтрализации угроз.	3 балла
В схеме отражено наличие защищаемых ресурсов, кратко описаны элементы функциональной области нейтрализации угроз. Допускаются незначительные неточности.	2 балла
В схеме отражено наличие защищаемых ресурсов, отражены элементы функциональной области нейтрализации угроз. Ответ не содержит грубых ошибок.	1 балл
Отсутствуют крупные блоки или связи между ними. Присутствуют грубые ошибки или неточности.	0 баллов

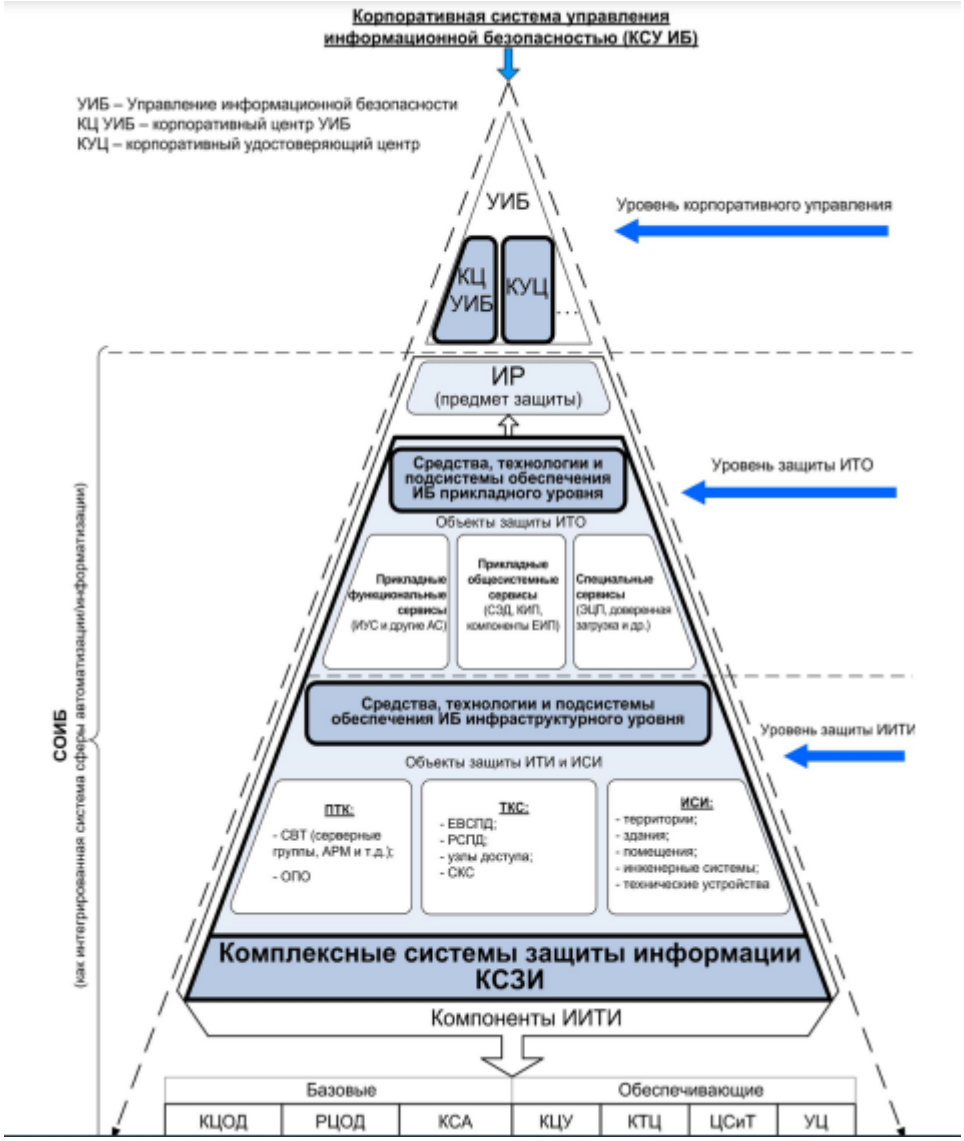
Примерное решение:



4. Нарисуйте общую схему архитектуры обеспечения информационной безопасности корпоративного предприятия.

Критерии оценивания	Шкала оценок
В схеме обозначены уровни системы обеспечения информационной безопасности (СОИБ), показана их структура, перечислены объекты защиты.	3 балла
В схеме обозначены уровни СОИБ, дано их описание, присутствуют примеры объектов защиты. Допускаются незначительные неточности.	2 балла
В схеме обозначены уровни СОИБ дано их описание. Ответ не содержит грубых ошибок.	1 балл
Отсутствуют уровни СОИБ. Присутствуют грубые ошибки или неточности.	0 баллов

Примерное решение:



5. Задана вероятность подбора пароля $P = 10^{-6}$. Необходимо найти минимальную длину пароля L, которая обеспечит его стойкость в течение одной недели непрерывных попыток подобрать пароль со скоростью интерактивного подбора паролей V = 10 паролей/мин.

Критерии оценивания	Шкала оценок
Вычислено значение S, с использованием соотношения $S=A^L$ определено значение L, зависящее от A, удовлетворяющее условию $A^L >= V*T / P$. Имеются пояснение относительно выбора конкретного значения A (мощности алфавита).	3 балла
Вычислено значение S, с использованием соотношения $S=A^L$ определено значение L, зависящее от A, удовлетворяющее условию $A^L >= V*T / P$. Не указано из каких соображений выбиралось значение A.	2 балла

Нет пояснений к решению, но ответ удовлетворяет соотношению $A^L >= V*T / P$.	1 балл
Отсутствует решение. Присутствуют грубые ошибки или неточности.	0 баллов

Примерное решение:

В течение недели можно перебрать V*T = 10*60*24*7 = 100800 паролей. Далее, учитывая, что параметры S, V, T и P связаны соотношением P = V*T/S, получаем $S = V*T / P = 100800/10^{-6} = 10^{11}$. Полученному значению S соответствуют пары: A = 26, L = 8 где A – мощность алфавита паролей (при использовании только латинских символов одного регистра).

Правильные ответы

Номер вопроса	Ответ (буква)
1.	д
2.	а,б
3.	а
4.	в
5.	б
6.	б
7.	в
8.	б
9.	б
10.	г
11.	б
12.	в
13.	б
14.	а
15.	б
16.	а
17.	а,в,д

18.	б
19.	а
20.	в

с коротким ответом

Номер вопроса	Ответ (буква)
1.	объект информатизации
2.	обеспечивающая
3.	информационного обеспечения
4.	несанкционированный доступ
5.	CVSS:3.1/AV:N/AC:L/PR:H/UI:N/S:U/C:H/I:H/A:L

Компетенция ОПК-12

Вопросы с выбором ответа

1. Какие из перечисленных информационных потоков относятся к штатным каналам информационного взаимодействия объекта информатизации с внешней средой?

а) информационный обмен в штатных режимах через глобальные и корпоративные компьютерные сети;

б) все виды электрической связи (телефонная, мобильная и т.д.);

в) штатные документальные потоки, связанные с документальным информационным взаимодействием, управлением, отчетностью и т.д.;

г) всё перечисленные информационные потоки.

2. Какие из перечисленных информационных потоков относятся к побочным информационным процессам взаимодействии объекта информатизации с внешней средой?

а) электромагнитные излучения технических средств обработки и передачи информации, при этом сигналы, несущие информацию, можно принять специальной аппаратурой;

б) все виды электрической связи (телефонная, мобильная и т.д.);

в) информационный обмен в штатных режимах через глобальные и корпоративные компьютерные сети;

г) выход информации за пределы объекта за счёт непродуманных действий служащих (некорректная реклама, бесконтрольное уничтожение отходов - носителей информации и т.д.);

д) всё перечисленные информационные потоки.

3. Сущность принципа комплексности защиты информации состоит в:

а) оптимальном использование различных методов, мер и средств защиты информации для нейтрализации угроз информации и поддержания заданного уровня защищенности информации, интеграции этих средств в единую технологически связанную и управляемую систему;

б) обеспечении непрерывного целенаправленного процесса, предполагающего принятие соответствующих мер на всех этапах жизненного цикла автоматизированной системы, начиная с самых ранних стадий проектирования, а не только на этапе ее эксплуатации;

в) обеспечении оптимального уровня защиты, при котором затраты, риск и размер возможного ущерба были бы приемлемыми;

г) обеспечении возможности варьирования уровнем защищенности и средствами защиты.

4. Сущность принципа непрерывности защиты информации состоит в:

а) оптимальном использование различных методов, мер и средств защиты информации для нейтрализации угроз информации и поддержания заданного уровня защищенности информации, интеграции этих средств в единую технологически связанную и управляемую систему;

б) обеспечении непрерывного целенаправленного процесса, предполагающего принятие соответствующих мер на всех этапах жизненного цикла автоматизированной системы, начиная с самых ранних стадий проектирования, а не только на этапе ее эксплуатации;

в) обеспечении оптимального уровня защиты, при котором затраты, риск и размер возможного ущерба были бы приемлемыми;

г) обеспечении возможности варьирования уровнем защищенности и средствами защиты.

5. Сущность разумной достаточности защиты информации состоит в:

а) оптимальном использование различных методов, мер и средств защиты информации для нейтрализации угроз информации и поддержания заданного уровня защищенности информации, интеграции этих средств в единую технологически связанную и управляемую систему;

б) обеспечении непрерывного целенаправленного процесса, предполагающего принятие соответствующих мер на всех этапах жизненного цикла автоматизированной системы, начиная с самых ранних стадий проектирования, а не только на этапе ее эксплуатации;

в) обеспечении оптимального уровня защиты, при котором затраты, риск и размер возможного ущерба были бы приемлемыми;

г) обеспечении возможности варьирования уровнем защищенности и средствами защиты.

6. Сущность принципа гибкости системы защиты информации состоит в:

а) оптимальном использование различных методов, мер и средств защиты информации для нейтрализации угроз информации и поддержания заданного уровня защищенности информации, интеграции этих средств в единую технологически связанную и управляемую систему;

б) обеспечении непрерывного целенаправленного процесса, предполагающего принятие соответствующих мер на всех этапах жизненного цикла автоматизированной системы, начиная с самых ранних стадий проектирования, а не только на этапе ее эксплуатации;

в) обеспечении оптимального уровня защиты, при котором затраты, риск и размер возможного ущерба были бы приемлемыми;

г) обеспечении возможности варьирования уровнем защищенности и средствами защиты.

7. Какие из перечисленных подсистем защиты информации объекта информатизации (ОИ)

относятся к группе защиты информации в информационной сфере ОИ?

а) подсистема секретного и конфиденциального делопроизводства;

б) подсистема защиты информации от несанкционированного доступа общесистемного инфраструктурного уровня;

в) подсистема предотвращения компьютерных атак в автоматизированных системах и ликвидации их последствий;

г) подсистема обеспечения целостности и сохранности информационных ресурсов;

д) подсистема защиты информации в каналах передачи данных на ОИ;

е) все перечисленные подсистемы.

8. Какая из перечисленных подсистем защиты информации объекта информатизации (ОИ) относится к группе защиты при внешнем информационном проявлении ОИ?

а) подсистема предотвращения скрытого внедрения в программные и технические средства программно-технического комплекса и телекоммуникационных сетей;

б) подсистема нейтрализации побочного информационного проявления ОИ;

в) подсистема предотвращения компьютерных атак в автоматизированных системах и ликвидации их последствий;

г) подсистема обеспечения целостности и сохранности информационных ресурсов;

д) подсистема защиты информации в каналах передачи данных на ОИ.

9. Какое из перечисленных определений соответствует понятию обеспечивающая подсистема комплексной системы защиты информации?

а) совокупность информационных ресурсов, средств и систем обработки информации, а также средств и систем жизнеобеспечения объекта информатизации, необходимых для установки и эксплуатации средств и систем обработки информации, реализации информационных технологий;

б) общесистемный структурный компонент комплексной системы защиты информации, предназначенный для постоянного поддержания заданного уровня информационной безопасности в автоматизированной системы и на объект информатизации и обеспечивающий эффективную реализацию процессов управления, скоординированных и взаимоувязанных с управлением информационными технологиями;

в) совокупность мер и средств реализации функциональных задач защиты информации, однородных по своей природе или относящихся к определенной сфере обеспечения условий для реализации функциональных задач защиты информации.

10. Какое из перечисленных определений соответствует понятию объект информатизации?

а) совокупность информационных ресурсов, средств и систем обработки информации, а также средств и систем жизнеобеспечения объекта информатизации, необходимых для установки и эксплуатации средств и систем обработки информации, реализации информационных технологий;

б) совокупность информационных ресурсов, средств и систем обработки информации, используемых в соответствии с заданной информационной технологией, а также средств их обеспечения, помещений или объектов (зданий, сооружений, технических средств), в которых эти средства и системы установлены, или помещений и объектов, предназначенных для ведения конфиденциальных переговоров;

в) общесистемный структурный компонент комплексной системы защиты информации,

предназначенный для постоянного поддержания заданного уровня информационной безопасности в автоматизированной системы и на объект информатизации и обеспечивающий эффективную реализацию процессов управления, скоординированных и взаимоувязанных с управлением информационными технологиями.

11. Какое из перечисленных определений соответствует понятию комплексная система защиты информации?

а) совокупность органов и (или) исполнителей, используемой ими техники защиты информации, а также объектов защиты информации, организованная и функционирующая по правилам и нормам, установленным соответствующими документами в области защиты информации;

б) совокупность информационных ресурсов, средств и систем обработки информации, а также средств и систем жизнеобеспечения объекта информатизации, необходимых для установки и эксплуатации средств и систем обработки информации, реализации информационных технологий;

в) совокупность мер и средств реализации функциональных задач защиты информации, однородных по своей природе или относящихся к определенной сфере обеспечения условий для реализации функциональных задач защиты информации;

12. К основным системным направлениям обеспечения защиты информации относятся:

а) организационная и инженерно-техническая защита ОИ для обеспечения информационной безопасности;

б) секретное и конфиденциальное делопроизводство;

в) защита от несанкционированного доступа к информации и ресурсам;

г) методы и средства криптографической защиты информации;

д) нормативно-правовое обеспечение информационной безопасности;

е) всё из перечисленного.

13. Какому понятию соответствует следующее определение: совокупность методов использования преобразований данных, направленных на то, чтобы сделать их бесполезными для противника?

а) шифрование;

б) дешифрование;

в) криптография.

14. Определение понятия несанкционированный доступ, согласно руководящим документам ФСТЭК России:

а) доступ к информации, нарушающий правила разграничения доступа с использованием штатных средств, предоставляемых средствами вычислительной техники или автоматизированными системами;

б) 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;

в) получение возможности обрабатывать данные, хранящиеся на различных носителях и накопителях, посредством самовольного изменения или фальсификации соответствующих прав и полномочий.

15. Какие последствия могут иметь место в результате несанкционированного доступа к информации?

а) реализация угрозы конфиденциальности информации;

б) реализация угрозы целостности информации;

в) раскрытие параметров системы;

г) всё перечисленное.

16. Какие способы несанкционированного доступа возможны, если источником конфиденциальной информации являются люди?

а) визуальное наблюдение, хищение, фотографирование;

б) копирование, модификация, сбор и аналитическая обработка;

в) перехват, хищение, уничтожение.

17. Какие способы несанкционированного доступа возможны, если источником конфиденциальной информации являются документы?

а) копирование, модификация, незаконное подключение;

б) визуальное наблюдение, хищение, фотографирование;

в) перехват, инициативное сотрудничество, уничтожение.

18. Какие способы несанкционированного доступа возможны, если источником конфиденциальной информации являются технические средства?

а) перехват, инициативное сотрудничество, уничтожение

б) копирование, модификация, незаконное подключение;

в) фотографирование, подслушивание переговоров, сбор и аналитическая обработка.

19. Какое понятие обозначает процедуру проверки подлинности:

а) авторизация;

б) аутентификация;

в) идентификация;

20. Каким требованиям должна удовлетворять хэш-функция, пригодная для использования в алгоритме цифровой подписи?

а) должна иметь возможность обрабатывать сообщения только определенной, фиксированной длины

б) результатом применения хэш-функции является хэш-код фиксированной длины;

в) обратное преобразование (нахождение сообщения x, имеющего заданный хэш-код) должна производиться относительно быстро;

г) вычисление хэш-функции от любого аргумента должно производиться относительно быстро.

21. Какова длина хэш-кода согласно Российскому стандарту на хэш-функцию (ГОСТ Р 34.11–94)?

а) 128 бит;

б) 256 бит;

в) 512 бит;

г) не регламентирована.

22. Как называется подход к реализации криптографической защиты, предполагающий частичную расшифровку зашифрованного файла, выполняемую для его фрагмента, который в данный момент использует прикладная программа?

а) предварительное шифрование;

б) динамическое шифрование;

в) статическое шифрование;

г) статистическое шифрование.

23. В компетенции какого ведомства находятся организационно-правовые и научно-технические проблемы синтеза и анализа средств криптографической защиты информации?

а) Межведомственная комиссия по защите государственной тайны;

б) Федеральная служба по техническому и экспортному контролю;

в) Федеральная служба безопасности.

24. Каким документом регламентируется правовая сторона разработки и использования средств криптографической защиты информации?

а) Указ Президента Российской Федерации от 03.04.95 № 334 с учетом принятых ранее законодательных и нормативных актов РФ;

б) Система сертификации средств криптографической защиты информации РОСС.RU.0001.030001;

в) Положение о сертификации средств защиты информации по требованиям безопасности информации.

25. Каким документом установлен порядок сертификации средств криптографической защиты информации?

а) Указ Президента Российской Федерации от 03.04.95 № 334 с учетом принятых ранее законодательных и нормативных актов РФ;

б) Система сертификации средств криптографической защиты информации РОСС.RU.0001.030001;

в) Положение о сертификации средств защиты информации по требованиям безопасности информации.

26. Какое ведомство сформировало банк данных угроз информационной безопасности?

а) Межведомственная комиссия по защите государственной тайны;

б) Федеральная служба по техническому и экспортному контролю;

в) Федеральная служба безопасности.

27. Какими основными свойствами характеризуется информация с точки зрения информационной безопасности?

а) целостность;

б) полнота;

в) доступность;

г) адекватность;

д) конфиденциальность;

е) секретность.

28. Какое определение характеризует свойство конфиденциальности информации?

а) состояние информации, при котором доступ к ней осуществляют только субъекты, имеющие на него право;

б) состояние информации, при котором отсутствует любое ее изменение либо изменение осуществляется только преднамеренно субъектами, имеющими на него право;

в) состояние информации, при котором субъекты, имеющие права доступа, могут реализовать их беспрепятственно.

29. Какое определение характеризует свойство целостности информации?

а) состояние информации, при котором доступ к ней осуществляют только субъекты, имеющие на него право;

б) состояние информации, при котором отсутствует любое ее изменение либо изменение осуществляется только преднамеренно субъектами, имеющими на него право;

в) состояние информации, при котором субъекты, имеющие права доступа, могут реализовать их беспрепятственно.

30. Какое определение характеризует свойство доступности информации?

а) состояние информации, при котором доступ к ней осуществляют только субъекты, имеющие на него право;

б) состояние информации, при котором отсутствует любое ее изменение либо изменение осуществляется только преднамеренно субъектами, имеющими на него право;

в) состояние информации, при котором субъекты, имеющие права доступа, могут реализовать их беспрепятственно.

Вопросы с коротким ответом

1. Впишите пропущенное слово: информационное взаимодействие объекта информатизации с внешней средой через различные неконтролируемые каналы (человеческий фактор, побочные электромагнитные излучения и виброакустические эффекты). – это … информационное проявление.

2. Какое понятие характеризуется следующим определением: совокупность информационных ресурсов, средств и систем обработки информации, используемых в соответствии с заданной информационной технологией, а также средств их обеспечения, помещений или объектов (зданий, сооружений, технических средств), в которых эти средства и системы установлены, или помещений и объектов, предназначенных для ведения конфиденциальных переговоров?

3. Какое понятие характеризуется следующим определением: совокупность органов и (или)

исполнителей, используемой ими техники защиты информации, а также объектов защиты информации, организованная и функционирующая по правилам и нормам, установленным соответствующими документами в области защиты информации?

4. Какая подсистема КСЗИ характеризуется следующим определением: совокупность мер и средств реализации функциональных задач защиты информации, однородных по своей природе или относящихся к определенной сфере обеспечения условий для реализации функциональных задач защиты информации?

5. Какая подсистема КСЗИ характеризуется следующим определением: совокупность норм, правил, регламентов и требований, устанавливающих на объекте информатизации и в процессах внешнего информационного обмена обязательный порядок информационных отношений между субъектами, отношений доступа субъектов к информационным объектам и к техническим ресурсам автоматизированной системы при работе с защищаемой информацией?

6. Как называется концептуальный документ объекта информатизации, содержащий совокупность документированных управленческих, организационных, технических и технологических решений, направленных на защиту информации и ассоциированных с ней других ресурсов с учетом утвержденной модели нарушителя?

7. Какая криптосистема основана на использовании одного и того же ключа как для шифрования, так и для дешифрования?

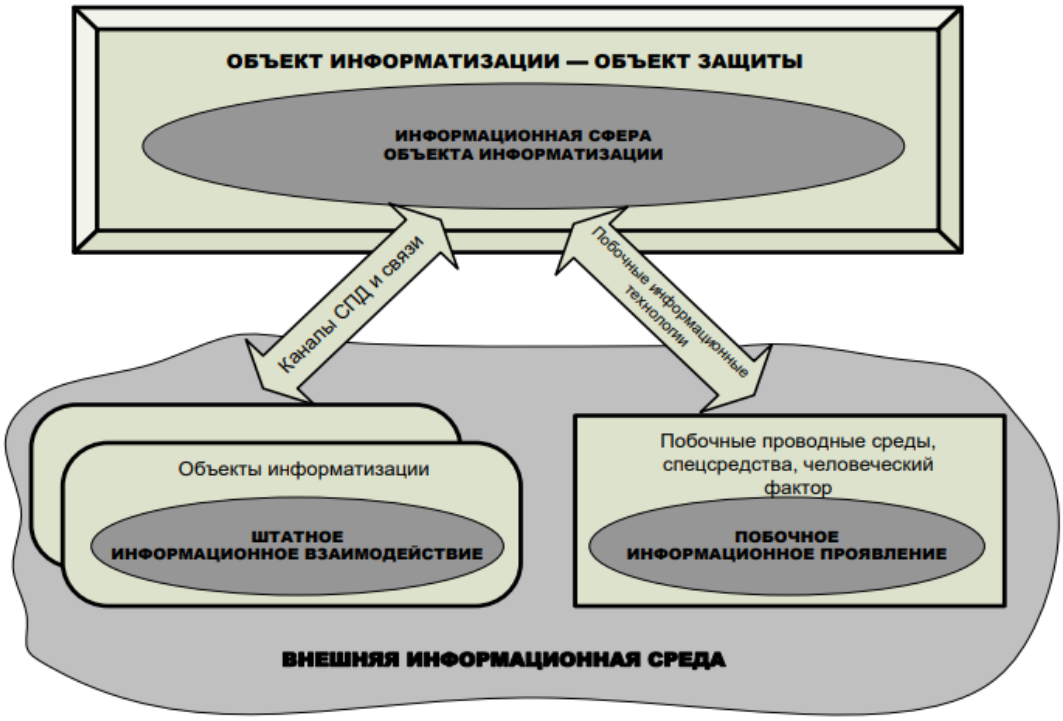
Вопросы с развернутым ответом

1. Нарисуйте структурную схему информационного представления объекта информатизации при взаимодействии с внешней средой.

Критерии оценивания	Шкала оценок
В схеме присутствуют блоки объекта информатизации (объект защиты), включающего внутреннюю информационную сферу, и внешней среды, включающей объекты штатного информационного взаимодействия (другие объекты информатизации) и средства, реализующие побочное информационное проявление. Обозначены штатные каналы передачи информации (системы передачи данных и связи, документооборот и т.п.) и побочные информационные потоки (процессы).	3 балла
В схеме присутствуют блоки объекта информатизации (объект защиты) и внешней среды, включающей объекты штатного информационного взаимодействия факторы побочного информационного проявления. Обозначены штатные каналы передачи информации (системы передачи данных и связи, документооборот и т.п.) и побочные информационные потоки (процессы). Допускаются незначительные неточности.	2 балла

В схеме присутствуют блоки объекта информатизации и внешней среды, обозначены элементы штатного и побочного информационного взаимодействия, обозначены соответствующие каналы передачи информации. Ответ не содержит грубых ошибок.	1 балл
Отсутствуют элементы штатного и побочного информационного взаимодействия объекта информатизации и внешней среды. Присутствуют грубые ошибки или неточности.	0 баллов

Примерное решение:

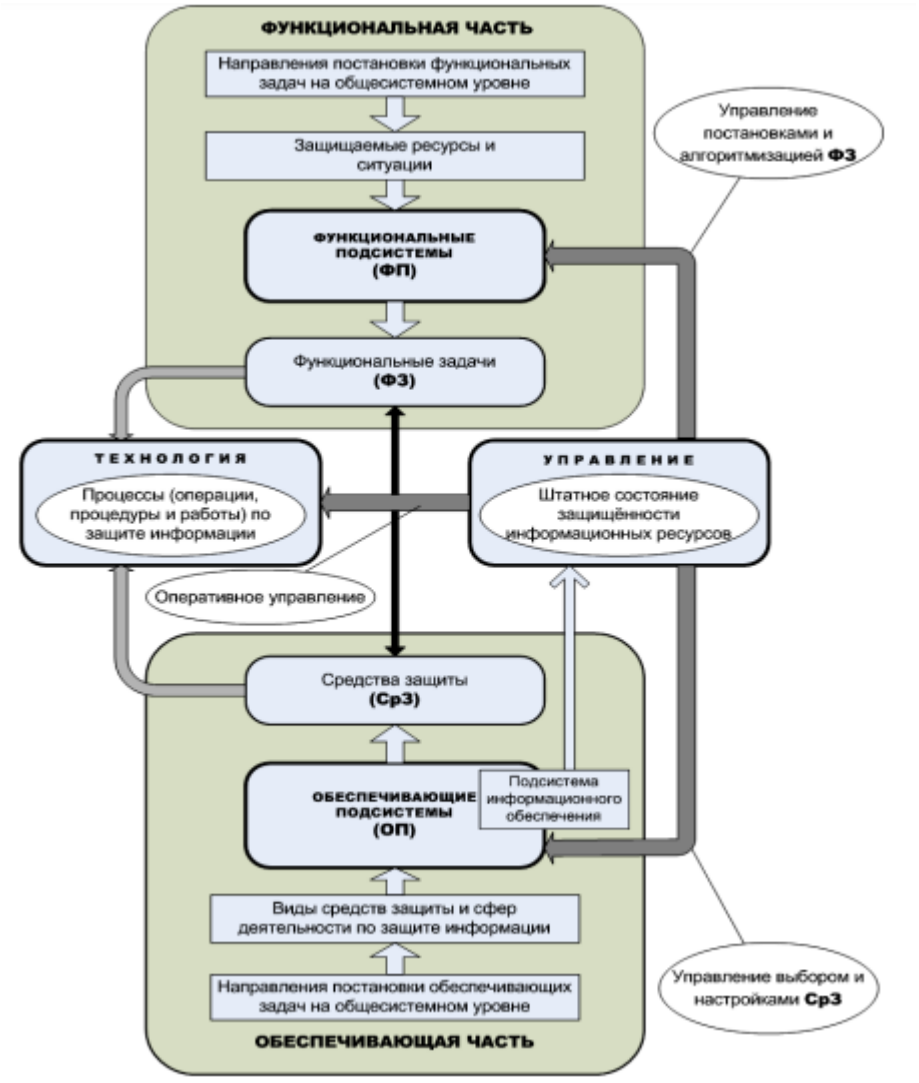


2. Нарисуйте структурную схему построения комплексной системы защиты на объекте информатизации.

Критерии оценивания	Шкала оценок
В схеме присутствуют блоки функциональной и обеспечивающих частей, связанные друг с другом и с компонентом технологии, а также компонент управления связывающий их все. В блоках функциональной и обеспечивающей частей отражены элементы синтеза функциональной и обеспечивающей подсистем защиты информации. Обозначены связи между структурными элементами.	3 балла

В схеме присутствуют блоки функциональной и обеспечивающих частей, связанные друг с другом и с компонентом технологии, а также компонент управления связывающий их все. В блоках функциональной и обеспечивающей частей присутствуют элементы функциональной и обеспечивающей подсистем защиты информации. Показаны связи между структурными элементами. Допускаются незначительные неточности.	2 балла
В схеме присутствуют все структурные компоненты. В блоках функциональной и обеспечивающей частей присутствуют элементы функциональной и обеспечивающей подсистем защиты информации. Показаны основные связи между структурными компонентами, без указания направления информационного взаимодействия. Ответ не содержит грубых ошибок.	1 балл
Отсутствуют структурные компоненты или большинство связей. Присутствуют грубые ошибки или неточности.	0 баллов

Примерное решение:

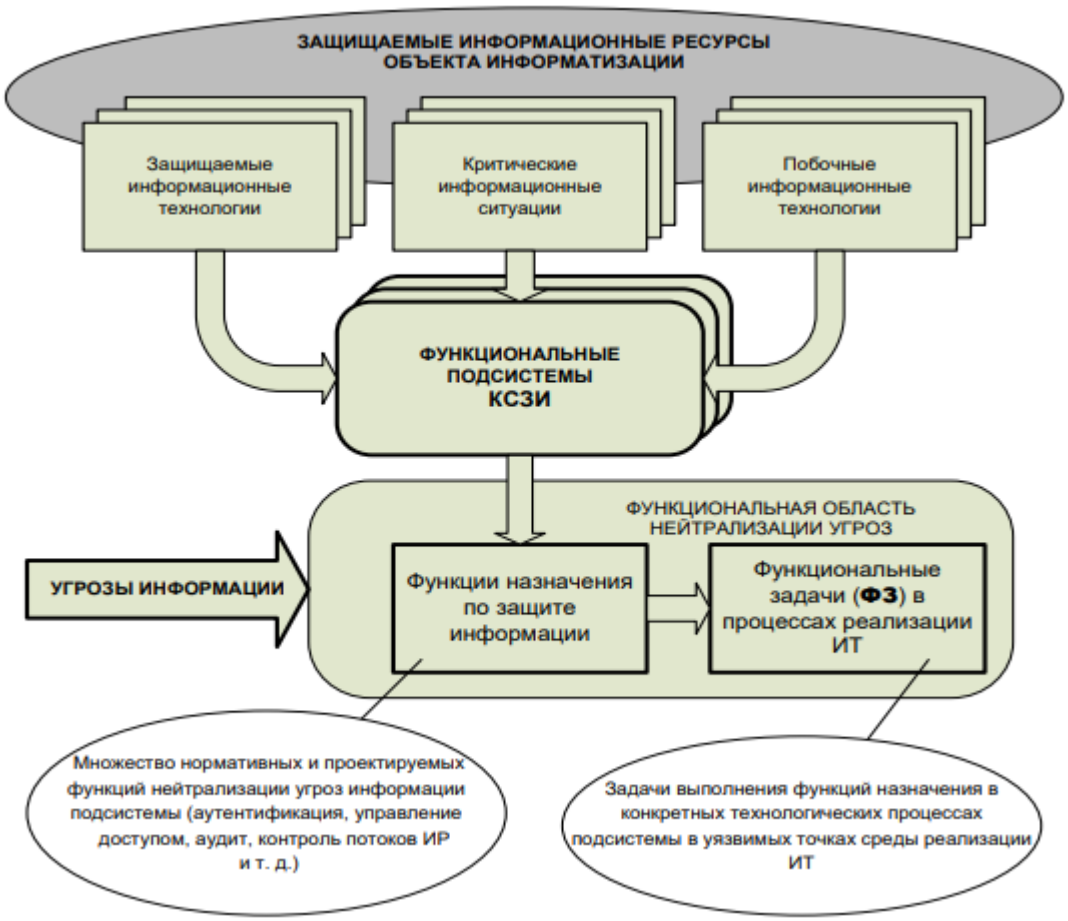


3. Нарисуйте схему формирования функциональных подсистем комплексной системы защиты на

объекте информатизации.

Критерии оценивания	Шкала оценок
В схеме обозначены основные защищаемые ресурсы, описаны элементы функциональной области нейтрализации угроз.	3 балла
В схеме отражено наличие защищаемых ресурсов, кратко описаны элементы функциональной области нейтрализации угроз. Допускаются незначительные неточности.	2 балла
В схеме отражено наличие защищаемых ресурсов, отражены элементы функциональной области нейтрализации угроз. Ответ не содержит грубых ошибок.	1 балл
Отсутствуют крупные блоки или связи между ними. Присутствуют грубые ошибки или неточности.	0 баллов

Примерное решение:

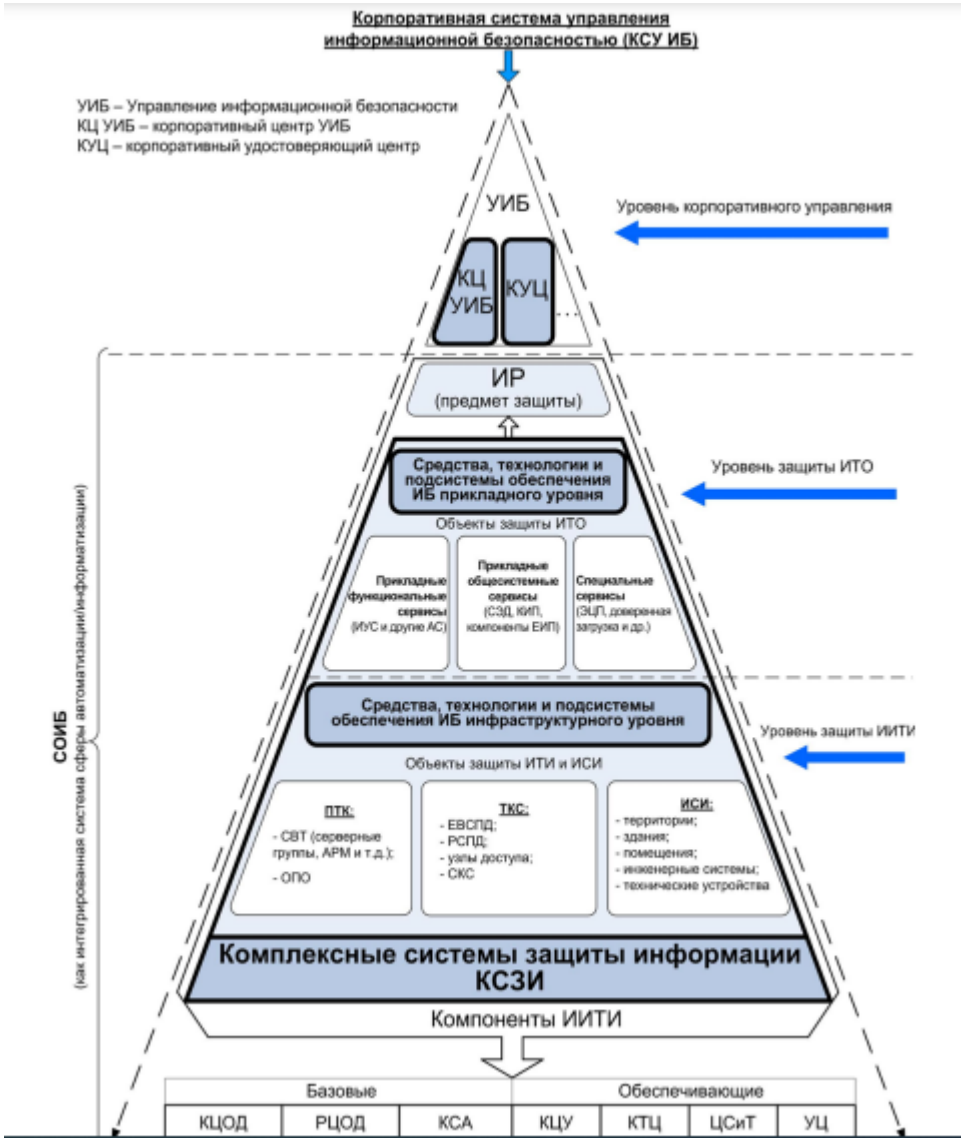


4. Нарисуйте общую схему архитектуры обеспечения информационной безопасности корпоративного предприятия.

Критерии оценивания	Шкала оценок

В схеме обозначены уровни системы обеспечения информационной безопасности (СОИБ), показана их структура, перечислены объекты защиты.	3 балла
В схеме обозначены уровни СОИБ, дано их описание, присутствуют примеры объектов защиты. Допускаются незначительные неточности.	2 балла
В схеме обозначены уровни СОИБ дано их описание. Ответ не содержит грубых ошибок.	1 балл
Отсутствуют уровни СОИБ. Присутствуют грубые ошибки или неточности.	0 баллов

Примерное решение:



5. Задана вероятность подбора пароля $P = 10^{-6}$. Необходимо найти минимальную длину пароля L, которая обеспечит его стойкость в течение одной недели непрерывных попыток подобрать пароль со скоростью интерактивного подбора паролей V = 10 паролей/мин.

Критерии оценивания	Шкала оценок
Вычислено значение S, с использованием соотношения $S=A^L$ определено значение L, зависящее от A, удовлетворяющее условию $A^L >= V*T / P$. Имеются пояснение относительно выбора конкретного значения A (мощности алфавита).	3 балла
Вычислено значение S, с использованием соотношения $S=A^L$ определено значение L, зависящее от A, удовлетворяющее условию $A^L >= V*T / P$. Не указано из каких соображений выбиралось значение A.	2 балла
Нет пояснений к решению, но ответ удовлетворяет соотношению $A^L >= V*T / P$.	1 балл
Отсутствует решение. Присутствуют грубые ошибки или неточности.	0 баллов

Примерное решение:

В течение недели можно перебрать $V*T = 10*60*24*7 = 100800$ паролей. Далее, учитывая, что параметры S, V, T и P связаны соотношением $P = V*T/S$, получаем $S = V*T / P = 100800/10^{-6} = 10^{11}$. Полученному значению S соответствует пара: A = 26, L = 8 где A – мощность алфавита паролей (при использовании только латинских символов одного регистра).

6. Задана вероятность подбора пароля $P = 10^{-5}$. Необходимо найти минимальную длину пароля L, которая обеспечит его стойкость в течение одной недели непрерывных попыток подобрать пароль со скоростью интерактивного подбора паролей V = 10 паролей/мин.

Критерии оценивания	Шкала оценок
Вычислено значение S, с использованием соотношения $S=A^L$ определено значение L, зависящее от A, удовлетворяющее условию $A^L >= V*T / P$. Имеются пояснение относительно выбора конкретного значения A (мощности алфавита).	3 балла
Вычислено значение S, с использованием соотношения $S=A^L$ определено значение L, зависящее от A, удовлетворяющее условию $A^L >= V*T / P$. Не указано из каких соображений выбиралось значение A.	2 балла
Нет пояснений к решению, но ответ удовлетворяет соотношению $A^L >= V*T / P$.	1 балл

Отсутствует решение. Присутствуют грубые ошибки или неточности.	0 баллов

Примерное решение:

В течение недели можно перебрать V*T = 10*60*24*7 = 100800 паролей. Далее, учитывая, что параметры S, V, T и P связаны соотношением P = V*T/S, получаем $S = V*T / P = 100800/10^{-5} = 10^{10}$. Полученному значению S соответствует пара: A = 36, L = 7 где A – мощность алфавита паролей (при использовании только латинских символов одного регистра и 10 цифр от 0 до 9).

7. Системные направления обеспечения защиты информации в АС на объекте информатизации.

Критерии оценивания	Шкала оценок
В ответе упомянуты все направления.	3 балла
Пропущено одно из направлений.	2 балла
Пропущено два или три направления.	1 балл
Отсутствуют четыре или более направлений.	0 баллов

Примерное решение:

1. Организационная и инженерно-техническая защита ОИ для обеспечения информационной безопасности (Режим и ИТЗ). 2. Секретное и конфиденциальное делопроизводство. 3. Защита от несанкционированного доступа к информации и ресурсам АС (Защита от НСД). 4. Методы и средства криптографической защиты информации в АС (СКЗИ). 5. Защита информации от несанкционированного копирования данных в среде АС (Защита от НСК). 6. Защита от скрытого внедрения в программно-техническую среду компьютерных и телекоммуникационных систем. 7. Защита информации от утечки по техническим каналам. 8. Нормативно-правовое обеспечение информационной безопасности.

Правильные ответы

Номер вопроса	Ответ (буква)
1.	г
2.	а,г
3.	а
4.	б
5.	в

6.	г
7.	е
8.	б
9.	в
10.	б
11.	а
12.	е
13.	в
14.	а
15.	г
16.	а
17.	б
18.	б
19.	б
20.	б,г
21.	б
22.	б
23.	в
24.	а
25.	б
26.	б
27.	а,в,д
28.	а
29.	б
30.	в

с коротким ответом

Номер вопроса	Ответ (буква)
1.	побочное
2.	объект информатизации
3.	комплексная система защиты информации
4.	обеспечивающая
5.	нормативно-правового обеспечения
6.	политика информационной безопасности
7.	симметричная