Министерство науки и высшего образования РФ
Федеральное государственное бюджетное образовательное учреждение высшего образования
«Заполярный государственный университет им. Н.М. Федоровского»
ЗГУ

ФОНД ОЦЕНОЧНЫХ СРЕДСТВ
по дисциплине
«*Анализ систем информационной безопасности*»

Факультет: *электроэнергетики, экономики и управления (ФЭЭиУ)*

Направление подготовки: *09.04.03 Прикладная информатика*

Профиль: *Информационные системы и технологии в бизнесе*

Уровень образования: *магистратура*

Кафедра «*Информационных систем и технологий*»
наименование кафедры

Разработчик ФОС:

доцент, к.т.н.,		А.М. Петров
(должность, степень, ученое звание)	(подпись)	(ФИО)

Оценочные материалы по дисциплине рассмотрены и одобрены на заседании кафедры, протокол № 01 от 30.09.2021 г.

Заведующий кафедрой _____ М.В. Петухов

Фонд оценочных средств по дисциплине «*Анализ систем информационной безопасности»* для текущей/промежуточной аттестации разработан в соответствии с Федеральным государственным образовательным стандартом высшего образования по *направлению подготовки 09.04.03 «Прикладная информатика»* на основе Рабочей программы дисциплины «*Анализ систем информационной безопасности»,* утвержденной решением ученого совета № 04-4/6 от 25.12.2020, Положения о формировании Фонда оценочных средств по дисциплине (ФОС), Положения о проведении текущего контроля успеваемости и промежуточной аттестации обучающихся ЗГУ, Положения о государственной итоговой аттестации (ГИА) выпускников по образовательным программам высшего образования в ЗГУ.

1. Перечень планируемых результатов обучения по дисциплине (модулю), соотнесенных с планируемыми результатами образовательной программы

Таблица 1 – Компетенции и индикаторы их достижения

Код и наименование компетенции	Индикаторы достижения и планируемые результаты обучения по дисциплине
Профессиональные	
ПК-3: Способен управлять процессами разработки программного обеспечения	ПК-3.1: Демонстрирует навыки управления процессами формирования и проверки требований к разрабатываемому программному обеспечению с учетом действующих правовых норм и законодательных актов
	ПК-3.3: Составляет планы процесса разработки программного продукта

Таблица 2. – Паспорт фонда оценочных средств

Контролируемые разделы (темы) дисциплины	**Формируемая компетенция**	**Наименование оценочного средства**	**Форма оценивания**
Введение в предмет	ПК- 3.1	Эссе, тестовые задания; экзаменационные билеты.	Устно/ письменно
Методики анализа ИС	ПК- 3.3	Эссе, тестовые задания; экзаменационные билеты.	Устно/ письменно
Анализ ИС ч.1.	ПК- 3.1	Эссе, тестовые задания; экзаменационные билеты.	Устно/ письменно
Анализ ИС ч.2.	ПК- 3.1	Эссе, тестовые задания; экзаменационные билеты.	Устно/ письменно
Анализ ИС ч.3.	ПК- 3.3	Эссе, тестовые задания; экзаменационные билеты.	Устно/ письменно
Анализ ИС ч.4.	ПК- 3.1	Эссе, тестовые задания; экзаменационные билеты.	Устно/ письменно
Самостоятельная работа	ПК- 3.3	Эссе, тестовые задания; экзаменационные билеты.	Устно/ письменно

Контролируемые разделы (темы) дисциплины	**Формируемая компетенция**	**Наименование оценочного средства**	**Форма оценивания**
Введение в предмет	ПК- 3.1	Эссе, тестовые задания; экзаменационные билеты.	Устно/ письменно
Методики анализа ИС	ПК- 3.3	Эссе, тестовые задания; экзаменационные билеты.	Устно/ письменно
Анализ ИС ч.1.	ПК- 3.1	Эссе, тестовые задания; экзаменационные билеты.	Устно/ письменно
Анализ ИС ч.2.	ПК- 3.1	Эссе, тестовые задания; экзаменационные билеты.	Устно/ письменно

Анализ ИС ч.3.	ПК- 3.3	Эссе, тестовые задания; экзаменационные билеты.	Устно/ письменно
Анализ ИС ч.4.	ПК- 3.1	Эссе, тестовые задания; экзаменационные билеты.	Устно/ письменно
Самостоятельная работа	ПК- 3.3	Эссе, тестовые задания; экзаменационные билеты.	Устно/ письменно

2. Перечень контрольно-оценочных средств (КОС)

Для определения качества освоения обучающимися учебного материала по дисциплине используются следующие контрольно-оценочные средства текущего контроля успеваемости, промежуточной аттестации обучающихся:

Таблица 3. Перечень контрольно-оценочных средств

	Наименование оценочного средства	**Сроки выполнения**	**Шкала оценивания**	**Критерии оценивания****
1.	***Текущий контроль качества ******			
	Тестовые задания	1 семестр	Достигнут/ не достигнут пороговый уровень освоения компетенции	Зачтено/ не зачтено
2.	Эссе			
	Промежуточная аттестация			
3.	Экзаменационные билеты	1 семестр	Освоил/ не освоил компетенцию*	Оценка**
	****Критерии оценки результатов обучения по дисциплине:** ***По 4-х бальной шкале:*** ***освоил компетенцию –*** *выставляется отметка отлично («5»), хорошо («4»), удовлетворительно («3»),* ***не освоил компетенцию-*** *выставляется отметка неудовлетворительно («2»).* ***Бинарная шкала:*** ***«зачтено» - освоил компетенцию;*** ***«не зачтено» - не освоил компетенцию.***			
	*** **Примерные виды оценочного средства текущей аттестации:** *в устной форме (устный опрос, защита письменной работы, доклад по результатам самостоятельной работы, проведение коллоквиумов, семинаров, решение ситуационных задач, защита лабораторных работ и т.д.);* *2) в письменной форме (письменный опрос, проверка выполнения письменных домашних заданий и расчетно-графических работ, написание рефератов, и т.д.).*			

*****Критерии промежуточной аттестации***

Критерии выставления оценки по 4-балльной шкале оценивания для экзамена или «зачтено с «оценкой»:

- оценки «отлично» заслуживает обучающийся, обнаруживший всесторонние, глубокие знания учебного материала и умение свободно выполнять задания, предусмотренные программой; изучивший основную литературу и знакомый с дополнительной литературой, рекомендованной программой обучения; безупречно отвечавший не только на вопросы билета, но и на дополнительные вопросы; проявивший творческие способности в использовании учебного материала;

- оценки «хорошо» заслуживает обучающийся, обнаруживший полные знания учебного материала, успешно выполнивший предусмотренные программой задания, изучивший основную литературу, отвечавший на все вопросы билета;

- оценки «удовлетворительно» заслуживает обучающийся, обнаруживший знания в объёме, необходимом для дальнейшей учёбы и работы по профессии, справившийся с выполнением заданий, знакомый с основной литературой, допустивший погрешности в ответе и при выполнении заданий, но обладающий достаточными знаниями для их устранения под руководством преподавателя;

- оценка «неудовлетворительно» выставляется обучающемуся, обнаружившему пробелы в знаниях основного учебного материала, допустившему принципиальные ошибки в выполнении предусмотренных рабочей программой заданий, которые не позволят ему продолжить обучение без дополнительных занятий по соответствующей дисциплине.

Критерии выставления аттестации «зачтено», «не зачтено»:

- **«Зачтено»** выставляется обучающемуся, если он показал достаточно прочные знания основных положений учебной дисциплины, умение самостоятельно решать конкретные практические задачи, предусмотренные рабочей программой, ориентироваться в рекомендованной справочной литературе, умеет правильно оценить полученные результаты.

- **«Не зачтено»** выставляется обучающемуся, если при ответе выявились существенные пробелы в знаниях основных положений учебной дисциплины, неумение с помощью преподавателя получить правильное решение конкретной практической задачи из числа предусмотренных рабочей программой учебной дисциплины.

3. Типовые контрольные задания или иные материалы, необходимые для оценки знаний, умений, навыков и (или) опыта деятельности, характеризующие процесс формирования компетенций в ходе освоения образовательной программы

3.1 Задания для текущего контроля успеваемости

«Эссе»

Темы:

1. Теория и методология обеспечения информационной безопасности и защиты информации.
2. Методы, аппаратно-программные и организационные средства защиты систем (объектов) формирования и предоставления пользователям информационных ресурсов различного вида.
3. Методы, модели и средства выявления, идентификации и классификации угроз нарушения информационной безопасности объектов различного вида и класса.
4. Системы документооборота (вне зависимости от степени их компьютеризации) и средства зашиты циркулирующей в них информации.
5. Методы и средства (комплексы средств) информационного противодействия угрозам нарушения информационной безопасности в открытых компьютерных сетях, включая Интернет.
6. Модели и методы формирования комплексов средств противодействия угрозам хищения (разрушения, модификации) информации и нарушения информационной безопасности для различного вида объектов защиты вне зависимости от области их функционирования.
7. Анализ рисков нарушения информационной безопасности и уязвимости процессов переработки информации в информационных системах любого вида и области применения.
8. Модели противодействия угрозам нарушения информационной безопасности для любого вида информационных систем.
9. Модели и методы оценки защищенности информации и информационной безопасности объекта.
10. Модели и методы оценки эффективности систем (комплексов) обеспечения информационной безопасности объектов защиты.
11. Технологии идентификации и аутентификации пользователей и субъектов информационных процессов. Системы разграничения доступа.
12. Мероприятия и механизмы формирования политики обеспечения информационной безопасности для объектов всех уровней иерархии системы управления.
13. Принципы и решения (технические, математические, организационные и др.) по

созданию новых и совершенствованию существующих средств защиты информации и обеспечения информационной безопасности.

14. Модели, методы и средства обеспечения внутреннего аудита и мониторинга состояния объекта, находящегося под воздействием угроз нарушения его информационной безопасности.

15. Модели и методы управления информационной безопасностью.

«Тестовые задания»

ОЦЕНОЧНОЕ СРЕДСТВО (тестирование)	**Контролируемая компетенция**
1) Кто является основным ответственным за определение уровня классификации информации? 1. Руководитель среднего звена; 2. Высшее руководство; 3. Владелец; 4. Пользователь;	**ПК 3.1**
2) Какая категория является наиболее рискованной для компании с точки зрения вероятного мошенничества и нарушения безопасности? 1. Сотрудники; 2. Хакеры; 3. Атакующие; 4. Контрагенты (лица, работающие по договору);	**ПК 3.1**
3) Если различным группам пользователей с различным уровнем доступа требуется доступ к одной и той же информации, какое из указанных ниже действий следует предпринять руководству? 1. Снизить уровень безопасности этой информации для обеспечения ее доступности и удобства использования; 2. Требовать подписания специального разрешения каждый раз, когда человеку требуется доступ к этой информации; 3. Улучшить контроль за безопасностью этой информации; 4. Снизить уровень классификации этой информации;	**ПК 3.1**
4) Что самое главное должно продумать руководство при классификации данных? 1. Типы сотрудников, контрагентов и клиентов, которые будут иметь доступ к данным; 2. Необходимый уровень доступности, целостности и конфиденциальности; 3. Оценить уровень риска и отменить контрмеры; 4. Управление доступом, которое должно защищать данные;	**ПК 3.1**
5) Кто в конечном счете несет ответственность за гарантии того, что данные классифицированы и защищены? 1. Владельцы данных; 2. Пользователи; 3. Администраторы; 4. Руководство;	**ПК 3.1**
6) Что такое процедура? 1. Правила использования программного и аппаратного обеспечения в компании; 2. Пошаговая инструкция по выполнению задачи; 3. Руководство по действиям в ситуациях, связанных с безопасностью, но не описанных в стандартах; 4. Обязательные действия;	**ПК 3.1**
7) Какой фактор наиболее важен для того, чтобы быть уверенным в успешном обеспечении безопасности в компании? а) Поддержка высшего руководства; б) Эффективные защитные меры и методы их внедрения; в) Актуальные и адекватные политики и процедуры безопасности; г) Проведение тренингов по безопасности для всех сотрудников;	**ПК 3.1**
8) Когда целесообразно не предпринимать никаких действий в отношении выявленных рисков?	**ПК 3.1**

1. Никогда. Для обеспечения хорошей безопасности нужно учитывать и снижать все риски; 2. Когда риски не могут быть приняты во внимание по политическим соображениям; 3. Когда необходимые защитные меры слишком сложны; 4. Когда стоимость контрмер превышает ценность актива и потенциальные потери;	
9) Что такое политики безопасности? 1. Пошаговые инструкции по выполнению задач безопасности; 2. Общие руководящие требования по достижению определенного уровня безопасности; 3. Широкие, высокоуровневые заявления руководства; 4. Детализированные документы по обработке инцидентов безопасности;	**ПК 3.1**
10) Какая из приведенных техник является самой важной при выборе конкретных защитных мер? 1. Анализ рисков; 2. Анализ затрат / выгоды; 3. Результаты ALE; 4. Выявление уязвимостей и угроз, являющихся причиной риска;	**ПК 3.1**
11) Что лучше всего описывает цель расчета ALE? 1. Количественно оценить уровень безопасности среды; 2. Оценить возможные потери для каждой контрмеры; 3. Количественно оценить затраты / выгоды; 4. Оценить потенциальные потери от угрозы в год;	**ПК 3.1**
12) Тактическое планирование – это: 1. Среднесрочное планирование; 2. Долгосрочное планирование; 3. Ежедневное планирование; 4. Планирование на 6 месяцев;	**ПК 3.1**
13) Что является определением воздействия (exposure) на безопасность? 1. Нечто, приводящее к ущербу от угрозы; 2. Любая потенциальная опасность для информации или систем; 3. Любой недостаток или отсутствие информационной безопасности; 4. Потенциальные потери от угрозы;	**ПК 3.1**
14) Эффективная программа безопасности требует сбалансированного применения: 1. Технических и нетехнических методов; 2. Контрмер и защитных механизмов; 3. Физической безопасности и технических средств защиты; 4. Процедур безопасности и шифрования;	**ПК 3.1**
15) Функциональность безопасности определяет ожидаемую работу механизмов безопасности, а гарантии определяют: 1. Внедрение управления механизмами безопасности; 2. Классификацию данных после внедрения механизмов безопасности; 3. Уровень доверия, обеспечиваемый механизмом безопасности; 4. Соотношение затрат / выгод;	**ПК 3.1**
16) Какое утверждение является правильным, если взглянуть на разницу в целях безопасности для коммерческой и военной организации? 1. Только военные имеют настоящую безопасность; 2. Коммерческая компания обычно больше заботится о целостности и доступности данных, а военные – о конфиденциальности; 3. Военным требуется больший уровень безопасности, т.к. их риски существенно выше; 4. Коммерческая компания обычно больше заботится о доступности и конфиденциальности данных, а военные – о целостности;	**ПК 3.1**
17) Как рассчитать остаточный риск? 1. Угрозы х Риски х Ценность актива; 2. (Угрозы х Ценность актива х Уязвимости) х Риски; 3. SLE х Частоту = ALE; 4. (Угрозы х Уязвимости х Ценность актива) х Недостаток контроля;	**ПК 3.1**

18) Что из перечисленного не является целью проведения анализа рисков? 1. Делегирование полномочий; 2. Количественная оценка воздействия потенциальных угроз; 3. Выявление рисков; 4. Определение баланса между воздействием риска и стоимостью необходимых контрмер;	**ПК 3.1**
19) Что из перечисленного не является задачей руководства в процессе внедрения и сопровождения безопасности? 1. Поддержка; 2. Выполнение анализа рисков; 3. Определение цели и границ; 4. Делегирование полномочий;	**ПК 3.1**
20) Почему при проведении анализа информационных рисков следует привлекать к этому специалистов из различных подразделений компании? 1. Чтобы убедиться, что проводится справедливая оценка; 2. Это не требуется. Для анализа рисков следует привлекать небольшую группу специалистов, не являющихся сотрудниками компании, что позволит обеспечить беспристрастный и качественный анализ; 3. Поскольку люди в различных подразделениях лучше понимают риски в своих подразделениях и смогут предоставить максимально полную и достоверную информацию для анализа; 4. Поскольку люди в различных подразделениях сами являются одной из причин рисков, они должны быть ответственны за их оценку;	**ПК 3.1**
21) Что является наилучшим описанием количественного анализа рисков? 1. Анализ, основанный на сценариях, предназначенный для выявления различных угроз безопасности; 2. Метод, используемый для точной оценки потенциальных потерь, вероятности потерь и рисков; 3. Метод, сопоставляющий денежное значение с каждым компонентом оценки рисков; 4. Метод, основанный на суждениях и интуиции;	**ПК 3.1**
22) Почему количественный анализ рисков в чистом виде не достижим? 1. Он достижим и используется; 2. Он присваивает уровни критичности. Их сложно перевести в денежный вид; 3. Это связано с точностью количественных элементов; 4. Количественные измерения должны применяться к качественным элементам;	**ПК 3.1**
23) Если используются автоматизированные инструменты для анализа рисков, почему все равно требуется так много времени для проведения анализа? 1. Много информации нужно собрать и ввести в программу; 2. Руководство должно одобрить создание группы; 3. Анализ рисков не может быть автоматизирован, что связано с самой природой оценки; 4. Множество людей должно одобрить данные;	**ПК 3.1**
24) Какой из следующих законодательных терминов относится к компании или человеку, выполняющему необходимые действия, и используется для определения обязательств? 1. Стандарты; 2. Должный процесс (Due process); 3. Должная забота (Due care); 4. Снижение обязательств;	**ПК 3.1**
25) Что такое CobiT и как он относится к разработке систем информационной безопасности и программ безопасности? 1. Список стандартов, процедур и политик для разработки программы безопасности; 2. Текущая версия ISO 17799;	**ПК 3.1**

3. Структура, которая была раз;работана для снижения внутреннего мошенничества в компаниях 4. Открытый стандарт, определяющий цели контроля;	
26) Из каких четырех доменов состоит CobiT? 1. Планирование и Организация, Приобретение и Внедрение, Эксплуатация и Сопровождение, Мониторинг и Оценка; 2. Планирование и Организация, Поддержка и Внедрение, Эксплуатация и Сопровождение, Мониторинг и Оценка; 3. Планирование и Организация, Приобретение и Внедрение, Сопровождение и Покупка, Мониторинг и Оценка; 4. Приобретение и Внедрение, Эксплуатация и Сопровождение, Мониторинг и Оценка;	**ПК 3.1**
27) Что представляет собой стандарт ISO/IEC 27799? 1. Стандарт по защите персональных данных о здоровье; 2. Новая версия BS 17799; 3. Определения для новой серии ISO 27000; 4. Новая версия NIST 800-60;	**ПК 3.1**
28) CobiT был разработан на основе структуры COSO. Что является основными целями и задачами COSO? 1. COSO – это подход к управлению рисками, который относится к контрольным объектам и бизнес-процессам; 2. COSO относится к стратегическому уровню, тогда как CobiT больше направлен на операционный уровень; 3. COSO учитывает корпоративную культуру и разработку политик; 4. COSO – это система отказоустойчивости;	**ПК 3.1**
29) OCTAVE, NIST 800-30 и AS/NZS 4360 являются различными подходами к реализации управления рисками в компаниях. В чем заключаются различия между этими методами? 1. NIST и OCTAVE являются корпоративными; 2. NIST и OCTAVE ориентирован на ИТ; 3. AS/NZS ориентирован на ИТ; 4. NIST и AS/NZS являются корпоративными;	**ПК 3.1**
Вопрос 30: Какой из следующих методов анализа рисков пытается определить, где вероятнее всего произойдет сбой? 1. Анализ связующего дерева; 2. AS/NZS; 3. NIST; 4. Анализ сбоев и дефектов;	**ПК 3.1**
31) Что было разработано, чтобы помочь странам и их правительствам построить законодательство по защите персональных данных похожим образом? 1. Безопасная OECD; 2. ISOIEC; 3. OECD; 4. CPTED;	**ПК 3.3**
32) Символы шифруемого текста перемещаются по определенным правилам внутри шифруемого блока этого текста, это метод: 1. Гаммирования; 2. Подстановки; 3. Кодирования; 4. Перестановки; 5. Аналитических преобразований;	**ПК 3.3**
33) Символы шифруемого текста последовательно складываются с символами некоторой специальной последовательности, это метод: 1. Гаммирования; 2. Подстановки; 3. Кодирования; 4. Перестановки; 5. Аналитических преобразований;	**ПК 3.3**
34) Защита информации от утечки это деятельность по предотвращению:	**ПК 3.3**

1. Получения защищаемой информации заинтересованным субъектом с нарушением установленных правовыми документами или собственником, владельцем информации прав или правил доступа к защищаемой информации; 2. Воздействия с нарушением установленных прав и/или правил на изменение информации, приводящего к искажению, уничтожению, копированию, блокированию доступа к информации, а также к утрате, уничтожению или сбою функционирования носителя информации; 3. Воздействия на защищаемую информацию ошибок пользователя информацией, сбоя технических и программных средств информационных систем, а также природных явлений; 4. Неконтролируемого распространения защищаемой информации от ее разглашения, несанкционированного доступа; 5. Несанкционированного доведения защищаемой информации до неконтролируемого количества получателей информации;	
35) Защита информации это: 1. Процесс сбора, накопления, обработки, хранения, распределения и поиска информации; 2. Преобразование информации, в результате которого содержание информации становится непонятным для субъекта, не имеющего доступа; 3. Получение субъектом возможности ознакомления с информацией, в том числе при помощи технических средств; 4. Совокупность правил, регламентирующих порядок и условия доступа субъекта к информации и ее носителям; 5. Деятельность по предотвращению утечки информации, несанкционированных и непреднамеренных воздействий на неё;	**ПК 3.3**
36) Естественные угрозы безопасности информации вызваны: 1. Деятельностью человека; 2. Ошибками при проектировании АСОИ, ее элементов или разработке программного обеспечения; 3. Воздействиями объективных физических процессов или стихийных природных явлений, независящих от человека; 4. Корыстными устремлениями злоумышленников; 5. Ошибками при действиях персонала;	**ПК 3.3**
37) К основным непреднамеренным искусственным угрозам АСОИ относится: 1. физическое разрушение системы путем взрыва, поджога и т.п.; 2. перехват побочных электромагнитных, акустических и других излучений устройств и линий связи; 3. изменение режимов работы устройств или программ, забастовка, саботаж персонала, постановка мощных активных помех и т.п.; 4. чтение остаточной информации из оперативной памяти и с внешних запоминающих устройств; 5. неумышленные действия, приводящие к частичному или полному отказу системы или разрушению аппаратных, программных, информационных ресурсов системы;	**ПК 3.3**
38) К посторонним лицам нарушителям информационной безопасности относится: 1. Представители организаций, взаимодействующих по вопросам обеспечения жизнедеятельности организации; 2. Персонал, обслуживающий технические средства; 3. Технический персонал, обслуживающий здание; 4. Пользователи; 5. Сотрудники службы безопасности; 6. Представители конкурирующих организаций; 7. Лица, нарушившие пропускной режим;	**ПК 3.3**
39) Спам, который имеет цель опорочить ту или иную фирму, компанию, политического кандидата и т.п: 1. Черный пиар; 2. Фишинг; 3. Нигерийские письма; 4. Источник слухов;	**ПК 3.3**

5. Пустые письма;	
40) Спам распространяет поддельные сообщения от имени банков или финансовых компаний, целью которых является сбор логинов, паролей и пин-кодов пользователей: 1. Черный пиар; 2. Фишинг; 3. Нигерийские письма; 4. Источник слухов; 5. Пустые письма;	**ПК 3.3**
41) Антивирус обеспечивает поиск вирусов в оперативной памяти, на внешних носителях путем подсчета и сравнения с эталоном контрольной суммы: 1. Детектор; 2. Доктор; 3. Сканер; 4. Ревизор; 5. Сторож;	**ПК 3.3**
42) Антивирус не только находит зараженные вирусами файлы, но и "лечит" их, т.е. удаляет из файла тело программы вируса, возвращая файлы в исходное состояние: 1. Детектор; 2. Доктор; 3. Сканер; 4. Ревизор; 5. Сторож;	**ПК 3.3**
43) Антивирус запоминает исходное состояние программ, каталогов и системных областей диска когда компьютер не заражен вирусом, а затем периодически или по команде пользователя сравнивает текущее состояние с исходным: 1. Детектор; 2. Доктор; 3. Сканер; 4. Ревизор; 5. Сторож;	**ПК 3.3**
44) Антивирус представляет собой небольшую резидентную программу, предназначенную для обнаружения подозрительных действий при работе компьютера, характерных для вирусов: 1. Детектор; 2. Доктор; 3. Сканер; 4. Ревизор; 5. Сторож;	**ПК 3.3**
45) Активный перехват информации это перехват, который: 1. Заключается в установке подслушивающего устройства в аппаратуру средств обработки информации; 2. Основан на фиксации электромагнитных излучений, возникающих при функционировании средств компьютерной техники и коммуникаций; 3. Неправомерно использует технологические отходы информационного процесса; 4. Осуществляется путем использования оптической техники; 5. Осуществляется с помощью подключения к телекоммуникационному оборудованию компьютера;	**ПК 3.3**
46) Перехват, который заключается в установке подслушивающего устройства в аппаратуру средств обработки информации называется: 1. Активный перехват; 2. Пассивный перехват; 3. Аудиоперехват; 4. Видеоперехват; 5. Просмотр мусора;	**ПК 3.3**
47) Перехват, который основан на фиксации электромагнитных излучений, возникающих при функционировании средств компьютерной техники и коммуникаций называется:	**ПК 3.3**

1. Активный перехват; 2. Пассивный перехват; 3. Аудиоперехват; 4. Видеоперехват; 5. Просмотр мусора;	
48) Перехват, который осуществляется путем использования оптической техники называется: 1. Активный перехват; 2. Пассивный перехват; 3. Аудиоперехват; 4. Видеоперехват; 5. Просмотр мусора;	**ПК 3.3**
49) К внутренним нарушителям информационной безопасности относится: 1. Клиенты; 2. Пользователи системы; 3. Посетители; 4. Любые лица, находящиеся внутри контролируемой территории; 5. Представители организаций, взаимодействующих по вопросам обеспечения жизнедеятельности организации. 6. Персонал, обслуживающий технические средства; 7. Сотрудники отделов разработки и сопровождения ПО; 8. Технический персонал, обслуживающий здание;	**ПК 3.3**
50) К правовым методам, обеспечивающим информационную безопасность, относятся: 1. Разработка аппаратных средств обеспечения правовых данных; 2. Разработка и установка во всех компьютерных правовых сетях журналов учета действий; 3. Разработка и конкретизация правовых нормативных актов обеспечения безопасности;	**ПК 3.3**
51) Основными источниками угроз информационной безопасности являются все указанное в списке: 1. Хищение жестких дисков, подключение к сети, инсайдерство; 2. Перехват данных, хищение данных, изменение архитектуры системы; 3. Хищение данных, подкуп системных администраторов, нарушение регламента работы;	**ПК 3.3**
52) Виды информационной безопасности: 1. Персональная, корпоративная, государственная 2. Клиентская, серверная, сетевая 3. Локальная, глобальная, смешанная	**ПК 3.3**
53) Цели информационной безопасности – своевременное обнаружение, предупреждение: 1. Несанкционированного доступа, воздействия в сети 2. Инсайдерства в организации 3. Чрезвычайных ситуаций	**ПК 3.3**
54) Основные объекты информационной безопасности: 1. Компьютерные сети, базы данных 2. Информационные системы, психологическое состояние пользователей 3. Бизнес-ориентированные, коммерческие системы	**ПК 3.3**
55) Основными рисками информационной безопасности являются: 1. Искажение, уменьшение объема, перекодировка информации 2. Техническое вмешательство, выведение из строя оборудования сети 3. Потеря, искажение, утечка информации	**ПК 3.3**
56) К основным принципам обеспечения информационной безопасности относится: 1. Экономической эффективности системы безопасности 2. Многоплатформенной реализации системы 3. Усиления защищенности всех звеньев системы	**ПК 3.3**
57) Основными субъектами информационной безопасности являются: 1. Руководители, менеджеры, администраторы компаний 2. Органы права, государства, бизнеса	**ПК 3.3**

3. Сетевые базы данных, фаерволлы	
58) К основным функциям системы безопасности можно отнести все перечисленное: 1. Установление регламента, аудит системы, выявление рисков 2. Установка новых офисных приложений, смена хостинг-компании 3. Внедрение аутентификации, проверки контактных данных пользователей	**ПК 3.3**
59) Принципом информационной безопасности является принцип недопущения: 1. Неоправданных ограничений при работе в сети (системе) 2. Рисков безопасности сети, системы 3. Презумпции секретности	**ПК 3.3**
60) Анализ систем информационной безопасности экономических систем позволяет оценить _____ уязвимостей и рисков.	**ПК 3.1**
61) В рамках анализа систем информационной безопасности используются различные методы и _____ для обнаружения уязвимостей.	**ПК 3.1**
62) Одной из основных целей анализа систем информационной безопасности является обеспечение _____ защиты данных и ресурсов.	**ПК 3.1**
63) Анализ систем информационной безопасности позволяет идентифицировать и _____ потенциальные угрозы.	**ПК 3.1**
64) Для эффективного анализа систем информационной безопасности необходимо проведение _____ уязвимостей и атак.	**ПК 3.1**
65) Анализ систем информационной безопасности включает оценку _____ существующих защитных мер и политик.	**ПК 3.1**
66) При проведении анализа систем информационной безопасности учитываются _____ внешней и внутренней среды.	**ПК 3.1**
67) Анализ систем информационной безопасности помогает определить оптимальные _____ для защиты данных.	**ПК 3.1**
68) Для успешного анализа систем информационной безопасности необходима комплексная _____ информации и данных.	**ПК 3.1**
69) Анализ систем информационной безопасности позволяет выявить _____ и уязвимые места в инфраструктуре	**ПК 3.1**
70) В рамках анализа систем информационной безопасности проводится оценка _____ безопасности и целостности данных.	**ПК 3.3**
71) Анализ систем информационной безопасности позволяет определить _____ для минимизации рисков.	**ПК 3.3**
72) При анализе систем информационной безопасности проводится оценка _____ доступа к информации и ресурсам.	**ПК 3.3**
73) Анализ систем информационной безопасности позволяет определить уровень _____ при обнаружении и реагировании на инциденты.	**ПК 3.3**
74) В рамках анализа систем информационной безопасности рассматриваются различные _____ нарушений безопасности.	**ПК 3.3**
75) Анализ систем информационной безопасности включает оценку _____ и целостности архитектуры системы.	**ПК 3.3**
76) При анализе систем информационной безопасности учитывается соответствие системы _____ и регуляторным требованиям.	**ПК 3.3**
77) Анализ систем информационной безопасности позволяет определить необходимые _____ для устранения уязвимостей.	**ПК 3.3**
78) В рамках анализа систем информационной безопасности проводится оценка эффективности _____ механизмов защиты.	**ПК 3.3**
79) Анализ систем информационной безопасности позволяет разработать _____ план действий для повышения уровня безопасности.	**ПК 3.3**

Ключи к заданиям по дисциплине «Анализ систем информационной безопасности экономических систем»

1	3	41	1
2	1	42	2
3	3	43	4
4	2	44	5
5	4	45	5
6	2	46	3
7	1	47	2
8	4	48	4
9	3	49	7
10	2	50	3
11	4	51	2
12	1	52	1
13	1	53	1
14	1	54	1
15	3	55	3
16	2	56	1
17	4	57	2
18	1	58	1
19	2	59	1
20	3	60	уровень
21	3	61	инструменты
22	4	62	надежной
23	1	63	обнаружить
24	3	64	сканирования
25	4	65	эффективности
26	1	66	факторы
27	1	67	меры
28	2	68	анализа
29	2	69	уязвимости
30	4	70	уровня
31	3	71	рекомендации
32	4	72	прав
33	1	73	реагирования
34	4	74	типы
35	5	75	конфиденциальности
36	3	76	стандартам
37	5	77	меры
38	6	78	защитных
39	1	79	стратегический
40	2		

3.2 Задания для промежуточной аттестации

«Экзамен»

Министерство науки и высшего образования
Российской Федерации
Федеральное государственное бюджетное
образовательное учреждение высшего образования «Заполярный государственный университет
им. Н. М. Федоровского»
Факультет ЭЭиУ

Кафедра Информационных систем и технологий

Экзаменационный билет № 1
по дисциплине «Анализ систем информационной безопасности»
подготовка магистрантов направления
09.04.05 «Прикладная информатика»

1. Напишите определения следующих терминов: информация; конфиденциальность информации; информация конфиденциальная.
2. Перечислите и объясните основные виды информации ограниченного доступа.
3. Перечислите направления защиты информации на объекте, согласно ГОСТ Р 50922 – 2006 «Защита информации. Основные термины и определения»

Преподаватель Петров А.М.

Утверждено на заседании кафедры №1 от 30.09.21 г.

Министерство науки и высшего образования
Российской Федерации
Федеральное государственное бюджетное
образовательное учреждение высшего образования «Заполярный государственный университет
им. Н. М. Федоровского»
Факультет ЭЭиУ

Кафедра Информационных систем и технологий

Экзаменационный билет № 2
по дисциплине «Анализ систем информационной безопасности»
подготовка магистрантов направления
09.04.05 «Прикладная информатика»

1. Напишите определения следующих терминов: информационная безопасность; доступность информации; целостность информации.
2. Начертите и объясните классификацию видов угроз информационной безопасности.
3. Начертите и объясните классификацию средств защиты информации.

Преподаватель Петров А.М.

Утверждено на заседании кафедры №1 от 30.09.21 г.

Министерство науки и высшего образования
Российской Федерации
Федеральное государственное бюджетное
образовательное учреждение высшего образования «Заполярный государственный университет
им. Н. М. Федоровского»
Факультет ЭЭиУ

Кафедра Информационных систем и технологий

Экзаменационный билет № 3
по дисциплине «Анализ систем информационной безопасности»
подготовка магистрантов направления
09.04.05 «Прикладная информатика»

1. Начертите и объясните базовую модель передачи данных.
2. Перечислите существующие методы взлома.
3. Перечислите существующие методы криптоанализа.

Преподаватель Петров А.М.

Утверждено на заседании кафедры №1 от 30.09.21 г.

Министерство науки и высшего образования
Российской Федерации
Федеральное государственное бюджетное
образовательное учреждение высшего образования «Заполярный государственный университет
им. Н. М. Федоровского»
Факультет ЭЭиУ

Кафедра Информационных систем и технологий

Экзаменационный билет № 4
по дисциплине «Анализ систем информационной безопасности»
подготовка магистрантов направления
09.04.05 «Прикладная информатика»

1. Начертите и объясните жизненный цикл системы информационной безопасности.
2. Начертите и объясните классификацию источников информационных угроз для РФ.
3. Начертите и объясните классификацию основных видов информационных угроз.

Преподаватель Петров А.М.

Утверждено на заседании кафедры №1 от 30.09.21 г.

Министерство науки и высшего образования
Российской Федерации
Федеральное государственное бюджетное
образовательное учреждение высшего образования «Заполярный государственный университет
им. Н. М. Федоровского»
Факультет ЭЭиУ

Кафедра Информационных систем и технологий

Экзаменационный билет № 5
по дисциплине «Анализ систем информационной безопасности»
подготовка магистрантов направления
09.04.05 «Прикладная информатика»

1. Перечислите и объясните любые пять фундаментальных законов о информационной безопасности.
2. Перечислите национальные интересы РФ в информационной сфере с точки зрения ДИБ.
3. Перечислите негативные факторы, влияющие на состояние ИБ с точки зрения ДИБ.

Преподаватель Петров А.М.

Утверждено на заседании кафедры №1 от 30.09.21 г.

Министерство науки и высшего образования
Российской Федерации
Федеральное государственное бюджетное
образовательное учреждение высшего образования «Заполярный государственный университет
им. Н. М. Федоровского»
Факультет ЭЭиУ

Кафедра Информационных систем и технологий

Экзаменационный билет № 6
по дисциплине «Анализ систем информационной безопасности»
подготовка магистрантов направления
09.04.05 «Прикладная информатика»

1. Что такое манифест свободного информационного пространства и в чем его суть?
2. Начертите и объясните любую одну из четырех классификаций компьютерных вирусов.
3. Перечислите существующие программные средства защиты информации.

Преподаватель Петров А.М.

Утверждено на заседании кафедры №1 от 30.09.21 г.

Министерство науки и высшего образования
Российской Федерации
Федеральное государственное бюджетное
образовательное учреждение высшего образования «Заполярный государственный университет
им. Н. М. Федоровского»
Факультет ЭЭиУ

Кафедра Информационных систем и технологий

Экзаменационный билет № 7
по дисциплине «Анализ систем информационной безопасности»
подготовка магистрантов направления
09.04.05 «Прикладная информатика»

1. Напишите определения следующих терминов: информация; конфиденциальность информации; информация конфиденциальная.
2. Начертите и объясните любую одну из четырех классификаций компьютерных вирусов.
3. Начертите и объясните любую одну из четырех классификаций компьютерных вирусов.

Преподаватель Петров А.М.

Утверждено на заседании кафедры №1 от 30.09.21 г.

Министерство науки и высшего образования
Российской Федерации
Федеральное государственное бюджетное
образовательное учреждение высшего образования «Заполярный государственный университет
им. Н. М. Федоровского»
Факультет ЭЭиУ

Кафедра Информационных систем и технологий

Экзаменационный билет № 8
по дисциплине «Анализ систем информационной безопасности»
подготовка магистрантов направления
09.04.05 «Прикладная информатика»

1. Напишите определения следующих терминов: информационная безопасность; доступность информации; целостность информации.
2. Начертите и объясните классификацию видов угроз информационной безопасности.
3. Начертите и объясните классификацию средств защиты информации.

Преподаватель Петров А.М.

Утверждено на заседании кафедры №1 от 30.09.21 г.

Министерство науки и высшего образования
Российской Федерации
Федеральное государственное бюджетное
образовательное учреждение высшего образования «Заполярный государственный университет
им. Н. М. Федоровского»
Факультет ЭЭиУ

Кафедра Информационных систем и технологий

Экзаменационный билет № 9
по дисциплине «Анализ систем информационной безопасности»
подготовка магистрантов направления
09.04.05 «Прикладная информатика»

1. Напишите определения следующих терминов: информация; конфиденциальность информации; информация конфиденциальная.
2. Перечислите существующие методы взлома.
3. Перечислите существующие методы криптоанализа.

Преподаватель Петров А.М.

Утверждено на заседании кафедры №1 от 30.09.21 г.

Министерство науки и высшего образования
Российской Федерации
Федеральное государственное бюджетное
образовательное учреждение высшего образования «Заполярный государственный университет
им. Н. М. Федоровского»
Факультет ЭЭиУ

Кафедра Информационных систем и технологий

Экзаменационный билет № 10
по дисциплине «Анализ систем информационной безопасности»
подготовка магистрантов направления
09.04.05 «Прикладная информатика»

1. Начертите и объясните жизненный цикл системы информационной безопасности.
2. Начертите и объясните классификацию источников информационных угроз для РФ.
3. Начертите и объясните любую одну из четырех классификаций компьютерных вирусов.

Преподаватель Петров А.М.

Утверждено на заседании кафедры №1 от 30.09.21 г.

Министерство науки и высшего образования
Российской Федерации
Федеральное государственное бюджетное
образовательное учреждение высшего образования «Заполярный государственный университет
им. Н. М. Федоровского»
Факультет ЭЭиУ

Кафедра Информационных систем и технологий

Экзаменационный билет № 11
по дисциплине «Анализ систем информационной безопасности»
подготовка магистрантов направления
09.04.05 «Прикладная информатика»

1. Перечислите и объясните любые пять фундаментальных законов о информационной безопасности.
2. Перечислите национальные интересы РФ в информационной сфере с точки зрения ДИБ.
3. Перечислите негативные факторы, влияющие на состояние ИБ с точки зрения ДИБ.

Преподаватель Петров А.М.

Утверждено на заседании кафедры №1 от 30.09.21 г.

Министерство науки и высшего образования
Российской Федерации
Федеральное государственное бюджетное
образовательное учреждение высшего образования «Заполярный государственный университет
им. Н. М. Федоровского»
Факультет ЭЭиУ

Кафедра Информационных систем и технологий

Экзаменационный билет № 12
по дисциплине «Анализ систем информационной безопасности»
подготовка магистрантов направления
09.04.05 «Прикладная информатика»

1. Напишите определения следующих терминов: информация; конфиденциальность информации; информация конфиденциальная.
2. Перечислите национальные интересы РФ в информационной сфере с точки зрения ДИБ.
3. Начертите и объясните любую одну из четырех классификаций компьютерных вирусов.

Преподаватель Петров А.М.

Утверждено на заседании кафедры №1 от 30.09.21 г.

Министерство науки и высшего образования
Российской Федерации
Федеральное государственное бюджетное
образовательное учреждение высшего образования «Заполярный государственный университет
им. Н. М. Федоровского»
Факультет ЭЭиУ

Кафедра Информационных систем и технологий

Экзаменационный билет № 13
по дисциплине «Анализ систем информационной безопасности»
подготовка магистрантов направления
09.04.05 «Прикладная информатика»

1. Напишите определения следующих терминов: информация; конфиденциальность информации; информация конфиденциальная.
2. Перечислите и объясните основные виды информации ограниченного доступа.
3. Перечислите направления защиты информации на объекте, согласно ГОСТ Р 50922 – 2006 «Защита информации. Основные термины и определения»

Преподаватель Петров А.М.

Утверждено на заседании кафедры №1 от 30.09.21 г.

Министерство науки и высшего образования
Российской Федерации
Федеральное государственное бюджетное
образовательное учреждение высшего образования «Заполярный государственный университет
им. Н. М. Федоровского»
Факультет ЭЭиУ

Кафедра Информационных систем и технологий

Экзаменационный билет № 14
по дисциплине «Анализ систем информационной безопасности»
подготовка магистрантов направления
09.04.05 «Прикладная информатика»

1. Напишите определения следующих терминов: информационная безопасность; доступность информации; целостность информации.
2. Перечислите национальные интересы РФ в информационной сфере с точки зрения ДИБ.
3. Начертите и объясните классификацию средств защиты информации.

Преподаватель Петров А.М.

Утверждено на заседании кафедры №1 от 30.09.21 г.

Министерство науки и высшего образования
Российской Федерации
Федеральное государственное бюджетное
образовательное учреждение высшего образования «Заполярный государственный университет
им. Н. М. Федоровского»
Факультет ЭЭиУ

Кафедра Информационных систем и технологий

Экзаменационный билет № 15
по дисциплине «Анализ систем информационной безопасности»
подготовка магистрантов направления
09.04.05 «Прикладная информатика»

1. Начертите и объясните базовую модель передачи данных.
2. Перечислите существующие методы взлома.
3. Начертите и объясните любую одну из четырех классификаций компьютерных вирусов.

Преподаватель Петров А.М.

Утверждено на заседании кафедры №1 от 30.09.21 г.

Министерство науки и высшего образования
Российской Федерации
Федеральное государственное бюджетное
образовательное учреждение высшего образования «Заполярный государственный университет
им. Н. М. Федоровского»
Факультет ЭЭиУ

Кафедра Информационных систем и технологий

Экзаменационный билет № 16
по дисциплине «Анализ систем информационной безопасности»
подготовка магистрантов направления
09.04.05 «Прикладная информатика»

1. Напишите определения следующих терминов: информация; конфиденциальность информации; информация конфиденциальная.
2. Начертите и объясните классификацию источников информационных угроз для РФ.
3. Начертите и объясните классификацию основных видов информационных угроз.

Преподаватель Петров А.М.

Утверждено на заседании кафедры №1 от 30.09.21 г.

Министерство науки и высшего образования
Российской Федерации
Федеральное государственное бюджетное
образовательное учреждение высшего образования «Заполярный государственный университет
им. Н. М. Федоровского»
Факультет ЭЭиУ

Кафедра Информационных систем и технологий

Экзаменационный билет № 17
по дисциплине «Анализ систем информационной безопасности»
подготовка магистрантов направления
09.04.05 «Прикладная информатика»

1. Перечислите и объясните любые пять фундаментальных законов о информационной безопасности.
2. Перечислите национальные интересы РФ в информационной сфере с точки зрения ДИБ.
3. Начертите и объясните любую одну из четырех классификаций компьютерных вирусов.

Преподаватель Петров А.М.

Утверждено на заседании кафедры №1 от 30.09.21 г.

Министерство науки и высшего образования
Российской Федерации
Федеральное государственное бюджетное
образовательное учреждение высшего образования «Заполярный государственный университет
им. Н. М. Федоровского»
Факультет ЭЭиУ

Кафедра Информационных систем и технологий

Экзаменационный билет № 18
по дисциплине «Анализ систем информационной безопасности»
подготовка магистрантов направления
09.04.05 «Прикладная информатика»

1. Напишите определения следующих терминов: информация; конфиденциальность информации; информация конфиденциальная.
2. Начертите и объясните любую одну из четырех классификаций компьютерных вирусов.
3. Перечислите национальные интересы РФ в информационной сфере с точки зрения ДИБ.

Преподаватель Петров А.М.

Утверждено на заседании кафедры №1 от 30.09.21 г.

Министерство науки и высшего образования
Российской Федерации
Федеральное государственное бюджетное
образовательное учреждение высшего образования «Заполярный государственный университет
им. Н. М. Федоровского»
Факультет ЭЭиУ

Кафедра Информационных систем и технологий

Экзаменационный билет № 19
по дисциплине «Анализ систем информационной безопасности»
подготовка магистрантов направления
09.04.05 «Прикладная информатика»

1. Система защиты информации - комплекс организационных и технических мероприятий по защите информации, проведенный на объекте с применением необходимых технических средств и способов в соответствии с концепцией, целью и замыслом защиты.
2. Концепция защиты информации – это система взглядов и общих технических требований по защите информации.
3. Цель защиты информации - заранее намеченный уровень защищенности информации, получаемый в результате реализации системы защиты на объекте.
4. Замысел защиты - основная идея, раскрывающая состав, содержание, взаимосвязь и последовательность мероприятий, необходимых для достижения цели защиты информации на объекте.

Преподаватель Петров А.М.

Утверждено на заседании кафедры №1 от 30.09.21 г.

Министерство науки и высшего образования
Российской Федерации
Федеральное государственное бюджетное
образовательное учреждение высшего образования «Заполярный государственный университет
им. Н. М. Федоровского»
Факультет ЭЭиУ

Кафедра Информационных систем и технологий

Экзаменационный билет № 20
по дисциплине «Анализ систем информационной безопасности»
подготовка магистрантов направления
09.04.05 «Прикладная информатика»

1. Техническое средство защиты информации - техническое средство, предназначенное для устранения или ослабления демаскирующих признаков объекта, создания ложных (имитирующих) признаков, а также для создания помех техническим средством доступа информации.
2. Способ защиты информации - прием (метод), используемый для организации защиты информации.
3. Технико-экономическое обоснование ЗИ - определение оптимального объема организационных и технических мероприятий в составе системы защиты информации на объекте, необходимого для достижения цели защиты.

Преподаватель Петров А.М.

Утверждено на заседании кафедры №1 от 30.09.21 г.