МИНОБРНАУКИ РОССИИ
федеральное государственное бюджетное образовательное учреждение высшего образования
«Самарский государственный технический университет»
(ФГБОУ ВО «СамГТУ»)

УТВЕРЖДАЮ:
Проректор по учебной работе

_____
(подпись, ФИО)
«____»_____20__ г.

РАБОЧАЯ ПРОГРАММА МОДУЛЯ

Основы защиты информации

УГСН	09.00.00 Информатика и вычислительная техника
Направление подготовки (специальность)	09.03.01 Информатика и вычислительная техника
Квалификация	*Бакалавр*
Форма обучения	*Очная*
Год начала подготовки	*2025*
Объем дисциплины, ч. / з.е. / недели	*108/3/2*
Образовательные технологии	*Традиционные*
Форма контроля (промежуточная аттестация)	*Семестр 1: Экзамен*
Подразделение – разработчик	*Кафедра «Информатика и вычислительная техника»*

Самара 2025

Основы защиты информации

Разработчик

Разработчик РПМ
Забержинский Борислав Эдуардович
Руководитель подразделения
Чуваков Александр Владимирович

СОДЕРЖАНИЕ

1. Перечень планируемых результатов обучения по модулю, соотнесенных с планируемыми результатами освоения образовательной программы 3

2. Место модуля в структуре образовательной программы 3

3. Объем модуля в зачетных единицах с указанием количества академических часов, выделенных на контактную работу обучающихся с преподавателем (по видам учебных занятий) и на самостоятельную работу обучающихся 4

4. Содержание модуля, структурированное по темам (разделам), с указанием отведенного на них количества академических часов и видов учебных занятий 5

4.1. Содержание лекционных занятий 6

4.2. Содержание лабораторных занятия 7

4.3. Содержание практических занятий 8

4.4. Содержание самостоятельной работы 9

5. Перечень учебной литературы и учебно-методического обеспечения по модулю 9

6. Перечень ресурсов информационно-телекоммуникационной сети «Интернет», профессиональных баз данных, информационно-справочных систем 10

7. Описание материально-технической базы, необходимой для осуществления образовательного процесса по модулю 10

ПРИЛОЖЕНИЕ 11

Фонд оценочных средств 11

1. Перечень планируемых результатов обучения по модулю, соотнесенных с планируемыми результатами освоения образовательной программы

Таблица 1

Наименование категории (группы) компетенций	**Код и наименование компетенции**	**Код и наименование индикатора достижения компетенции**	**Результаты обучения** (знать, уметь, владеть)
Профессиональные компетенции			
-	ПК-1 Способен анализировать и разрабатывать требования к программному обеспечению	ПК-1.1 Знает методы и приемы формализации задач, типовые решения, библиотеки программных модулей, возможности современных и перспективных средств разработки программных продуктов, технических средств	Знать методы и приемы формализации задач.
		ПК-1.2 Знает методологии и технологии проектирования и использования баз данных, разработки компьютерного программного обеспечения и технологии программирования	Знать методологии и технологии проектирования баз данных.
		ПК-1.3 Использует методы и средства проектирования программного обеспечения, структур и баз данных, существующие типовые решения и шаблоны проектирования компьютерного программного обеспечения	Уметь применять средства проектирования программного обеспечения.
		ПК-1.4 Проектирует структуры данных, баз данных, владеет сбором, систематизацией, выявлением взаимосвязей и документированием требований к компьютерному программному обеспечению	Владеть проектированием баз данных.
-	ПК-6 Способен осуществлять оценку соответствия требованиям существующих и проектируемых систем и сопровождать приемочные испытания и ввод в эксплуатацию	ПК-6.5 Владеет применением методов тестирования при выявлении и описании отклонений работы системы от требований	Владеть навыками тестирования систем.

2. Место модуля в структуре образовательной программы

Модуль входит в Вариативную часть.

Входные требования:

Предшествующие осваиваемые модули: Язык программирования C#, Язык программирования Java, Язык программирования JavaScript, Системный анализ и объектно-ориентированное проектирование, Разработка WEB приложений; *Последующие осваиваемые модули:* Математическое и имитационное моделирование, Нереляционные системы хранения данных, Методы и технологии искусственного интеллекта, Цифровая экономика, Практико-ориентированный проект.

3. Объем модуля в зачетных единицах с указанием количества академических часов, выделенных на контактную работу обучающихся с преподавателем (по видам учебных занятий) и на самостоятельную работу обучающихся

Таблица 3

Вид учебной работы	Всего часов	В том числе часов в электронной форме	В том числе часов в форме практической подготовки	Семестр 1 часов/часов в электронной форме/в форме практической подготовки
Аудиторная контактная работа (всего), в том числе:	**48**	**0**	**0**	**48**
лекционные занятия (ЛЗ)	16	0	0	16
лабораторные работы (ЛР)	32	0	0	32
практические занятия (ПЗ)	0	0	0	0
Внеаудиторная контактная работа, КСР	**3**	**0**	**0**	**3**
Самостоятельная работа (всего), в том числе:	**57**	**0**	**0**	**57**
Подготовка к лабораторным работам	*57*	*0*	*0*	*57*
ИТОГО: час.	**108**	**0**	**0**	**108**
ИТОГО: з.е.	**3.0**	**0.0**	**0.0**	**3.0**

4. Содержание модуля, структурированное по темам (разделам), с указанием отведенного на них количества академических часов и видов учебных занятий

Таблица 4

№ раздела	Наименование раздела дисциплины	Виды учебной нагрузки и их трудоемкость, часы				
		ЛЗ	**ЛР**	**ПЗ**	**СРС**	**Всего часов**
1.	Основы криптографии.	8	16	0	30	54
2.	Основы хеширования.	8	16	0	27	51
	КСР					*3*
	Итого:	*16*	*32*	*0*	*57*	*108*

4.1. Содержание лекционных занятий

Таблица 4.1

№ ЛЗ	Наименование раздела	Тема лекции	Содержание лекции (перечень дидактических единиц: рассматриваемых подтем, вопросов)	Количество часов	Количество часов в электронной форме
Семестр 1					
1.	Основы криптографии.	Основы классической криптографии.	Криптография и криптология. Классическая задача криптографии. Шифрование и дешифрование информации.	2	0
2.	Основы криптографии.	Основы криптографии.	Понятие криптографического ключа. Время жизни ключей.	2	0
3.	Основы криптографии.	Симметричные алгоритмы шифрования.	Обобщенная схема криптосистемы. Криптоаналитическая атака: виды и проблемы защиты.	2	0
4.	Основы криптографии.	Симметричные алгоритмы шифрования.	Криптографические алгоритмы. Классификация криптографических алгоритмов. Теоретическая, практическая и временная стойкость системы крип тографической защиты.	2	0
5.	Основы хеширования.	Криптографические системы защиты информации.	Причины появления асимметричных алгоритмов шифрования. Односторонние функции.	2	0
6.	Основы хеширования.	Алгоритм цифровой подписи.	Алгоритм цифровой подписи RSA. Алгоритмы цифровой подписи Эль-Гамаля и DSA. Отечественный стандарт цифровой подписи.	2	0
7.	Основы хеширования.	Электронная цифровая подпись.	Проблема аутентичности информации. Понятие электронной цифровой подписи. Атаки на электронную цифровую подпись. Схема цифровой подписи.	2	0
8.	Основы хеширования.	Хэш-функции.	Базовые процедуры реализации электронной цифровой подписи Однонаправленные хэш-функции. Алгоритм SHA безопасного хеширования. Хэш-функции на основе симметричных блочных алгоритмов. Отечественный стандарт хэш-функции.	2	0
			Итого за семестр:	*16*	*0*
			Итого:	**16**	**0**

4.2. Содержание лабораторных занятий

Таблица 4.2

№ ЛабЗ	Наименование раздела	Наименование лабораторной работы	Содержание лабораторной работы (перечень рассматриваемых дидактических единиц: подтем, вопросов)	Количество часов	Количество часов в электронной форме	Количество часов в форме практической подготовки
Семестр 1						
1.	Основы криптографии.	Помехоустойчивое шифрование информации.	Алгоритмы сжатия информации. Кодирование данных алгоритмом Хаффмана.	4	0	*0*
2.	Основы криптографии.	Алгоритмы сжатия информации.	Запись закодированного сообщения в бинарный файл и декодирование данных, закодированных алгоритмом	4	0	*0*

№ ЛабЗ	Наименование раздела	Наименование лабораторной работы	Содержание лабораторной работы (перечень рассматриваемых дидактических единиц: подтем, вопросов)	Количество часов	Количество часов в электронной форме	Количество часов в форме практической подготовки
			Хаффмана.			
3.	Основы криптографии.	Циклические коды.	Разработка алгоритмического и программного обеспечения, реализующее алгоритм CRC.	4	0	*0*
4.	Основы криптографии.	Частотный метод дешифрования шифров замены.	Исследование частотных методов криптографической защиты информации.	4	0	*0*
5.	Основы хеширования.	Электронная цифровая подпись.	Проблема аутентичности информации. Понятие электронной цифровой подписи. Атаки на электронную цифровую подпись.	4	0	*0*
6.	Основы хеширования.	Схема цифровой подписи.	Исследование схемы цифровой подписи.	4	0	*0*
7.	Основы хеширования.	Реализация электронной цифровой подписи.	Базовые процедуры реализации электронной цифровой подписи. Алгоритм цифровой подписи RSA. Алгоритмы цифровой подписи Эль-Гамаля и DSA. Отечественный стандарт цифровой подписи.	4	0	*0*
8.	Основы хеширования.	Однонаправленные хэш-функции.	Алгоритм SHA безопасного хеширования. Хэш-функции на основе симметричных блочных алгоритмов. Отечественный стандарт хэш-функции.	4	0	*0*
			Итого за семестр:	*32*	*0*	*0*
			Итого:	**32**	**0**	***0***

4.3. Содержание самостоятельной работы

Таблица 4.4

Наименование раздела	Вид самостоятельной работы	Содержание самостоятельной работы (перечень дидактических единиц: рассматриваемых подтем, вопросов)	Количество часов
Семестр 1			
Основы криптографии.	Подготовка к лабораторным работам	Изучение Симметричных и ассиметричных алгоритмов шифрования.	30
Основы хеширования.	Подготовка к лабораторным работам	Изучение принципов технологий реализации электронной цифровой подписи.	27
		Итого за семестр:	*57*
		Итого:	**57**

5. Перечень учебной литературы и учебно-методического обеспечения по модулю

Таблица 5

№ п/п	Библиографическое описание	Ресурс НТБ СамГТУ	Ссылка на ресурс
1.	Евдокимов, М.А. Введение в криптологию. Вероятностный подход : моногр. / М. А. Евдокимов, В. Л. Спицын, А. В. Спицын; Самар.гос.техн.ун-т, Высшая математика и	Электронная библиотека СамГТУ (ЭБС Политех)	http:// platform.samgtu.ru/ getinfo?

№ п/п	Библиографическое описание	Ресурс НТБ СамГТУ	Ссылка на ресурс
	прикладная информатика.- Самара, 2011.- 230 с.		uid=els_samgtu-elib-1923
2.	Прохорова, О.В. Информационная безопасность и защита информации : учебник / О. В. Прохорова; Самарский государственный технический университет, Самарский государственный архитектурно-строительный университет.- Самара, 2014.- 114 с.	Электронная библиотека СамГТУ (ЭБС Политех)	http:// platform.samgtu.ru/ getinfo? uid=els_samgtu-elib-4779

Доступ обучающихся к ЭР НТБ СамГТУ (elib.samgtu.ru) осуществляется посредством электронной информационной образовательной среды университета и сайта НТБ СамГТУ по логину и паролю.

6. Перечень ресурсов информационно-телекоммуникационной сети «Интернет», профессиональных баз данных, информационно-справочных систем

Таблица 6

№ п/п	Наименование	Ссылка на веб-страницу ресурса	Режим доступа
1.	*Информационная безопасность [Электронный ресурс]. - Электрон. текстовые, граф., зв. дан., Сайт в сети Интернет*	*http://bugtraq.ru/*	*Ресурсы открытого доступа*

7. Описание материально-технической базы, необходимой для осуществления образовательного процесса по модулю

Лекционные занятия проводятся в:

Корпус № 12/520 - Компьютерный класс (Аудитория на 20 посадочных мест оснащена следующими техническими средствами обучения и оборудованием: учебная мебель, доска аудиторная, проектор. 10 ПК AMD FX-4100 и 1 ноутбук Samsung NP 350E7. На ПК и ноутбуке установлены следующие операционные системы: операционная система Microsift Windows 10 на учебных ПК, Microsoft Windows 8 на ноутбуке; На учебных ПК установлено следующее программное обеспечение: офисный пакет Microsoft Office стандартный 2010, Pyton 3.9.6 (64bit), Project Expert 7 Tutorial, Deductor Academic, Google Chrome, MATLAB R2010a, Node.js, Microsoft SQL Server VSS Writer, K-Lite Codec Pack 16.3.0 Full, 7-zip. PostgreSQL 10, Notepad++, Oracle VM VirtualBox, Npcap, scilab, OpenJDK, Microsoft Edge, Microsoft SQL Server 2008 (64bit), NetBeans IDE 8.2, Wireshark 3.4.7 64-bit, Far Manager 3 x64, QT, Adobe Acrobat Reader DC - Russian. На ноутбуке установлено следующее программное обеспечение: Microsoft Office 2007, Google chrome, Mozilla Firefox, Foxit Reader, Far Manager, 7 zip.Обеспечено проводное подключение ПК к локальной сети и сети Интернет.).

Практические занятия не предусмотрены.

Самостоятельная работа проводятся в:

Корпус № 8/200 - Читальный зал (Аудитория на 70 посадочных мест оснащена следующими техническими средствами обучения и оборудованием: учебная мебель, столы учебные.).

Лабораторные занятия проводятся в:

Корпус № 12/520 - Компьютерный класс (Аудитория на 20 посадочных мест оснащена следующими техническими средствами обучения и оборудованием: учебная мебель, доска аудиторная, проектор. 10 ПК AMD FX-4100 и 1 ноутбук Samsung NP 350E7. На ПК и ноутбуке установлены следующие операционные системы: операционная система Microsift Windows 10 на учебных ПК, Microsoft Windows 8 на ноутбуке; На учебных ПК установлено следующее программное обеспечение: офисный пакет Microsoft Office стандартный 2010, Pyton 3.9.6 (64bit), Project Expert 7 Tutorial, Deductor Academic, Google Chrome, MATLAB R2010a, Node.js, Microsoft SQL Server VSS Writer, K-Lite Codec Pack 16.3.0 Full, 7-zip. PostgreSQL 10, Notepad++, Oracle VM VirtualBox, Npcap, scilab, OpenJDK, Microsoft Edge, Microsoft SQL Server 2008 (64bit), NetBeans IDE 8.2, Wireshark 3.4.7 64-bit, Far Manager 3 x64, QT, Adobe Acrobat Reader DC - Russian. На ноутбуке установлено следующее программное обеспечение: Microsoft Office 2007, Google chrome, Mozilla Firefox, Foxit Reader, Far Manager, 7 zip.Обеспечено проводное подключение ПК к локальной сети и сети Интернет.).

ПРИЛОЖЕНИЕ

Фонд оценочных средств

Фонд оценочных средств для текущего контроля успеваемости, промежуточной аттестации обучающихся по модулю

Настоящий Фонд оценочных средств (ФОС) по модулю Основы защиты информации является неотъемлемым приложением к рабочей программе модуля. На данный ФОС распространяются все реквизиты утверждения, представленные в рабочей программе модуля.

1. Перечень оценочных средств

Таблица 1

№ п/п	Оценочное средство	Краткая характеристика оценочного средства	Количество	Представление оценочного средства в ФОС
1	Отчёт по лабораторной работе	Оценка способности студента применить полученные ранее знания для проведения анализа, опыта, эксперимента и выполнения последующих расчетов, а также составления выводов.	8	Требования к содержанию и оформлению отчета
2	Контрольная точка в форме тестирования	Инструмент, с помощью которого преподаватель оценивает степень достижения студентом требуемых знаний, умений, навыков в формате рубежного контроля по итогам изучения разделов. Составление теста включает в себя создание выверенной системы вопросов, собственно процедуру проведения тестирования и способ измерения полученных результатов.	1	Спецификация тестов и примеры вариантов тестовых заданий

Раздел 2. Этапы формирования компетенций, соотнесенные с видами оценочных средств

Таблица 2

Контролируемые разделы модуля	Код и формулировка индикатора компетенции	Результат обучения	Оценочные средства	Номер оценочного средства
Основы криптографии.	ПК-1.1 Знает методы и приемы формализации задач, типовые решения, библиотеки программных модулей, возможности современных и перспективных средств разработки программных продуктов, технических средств	Знать методы и приемы формализации задач.	Отчёт по лабораторной работе	1-4
Основы криптографии.	ПК-1.2 Знает методологии и технологии проектирования и использования баз данных, разработки компьютерного программного обеспечения и	Знать методологии и технологии проектирования баз данных.	Контрольная точка в форме тестирования	1

Контролируемые разделы модуля	Код и формулировка индикатора компетенции	Результат обучения	Оценочные средства	Номер оценочного средства
	технологии программирования			
Основы хеширования.	ПК-1.3 Использует методы и средства проектирования программного обеспечения, структур и баз данных, существующие типовые решения и шаблоны проектирования компьютерного программного обеспечения	Уметь применять средства проектирования программного обеспечения.	Отчёт по лабораторной работе	5-6
Основы хеширования.	ПК-1.4 Проектирует структуры данных, баз данных, владеет сбором, систематизацией, выявлением взаимосвязей и документированием требований к компьютерному программному обеспечению	Владеть проектированием баз данных.	Отчёт по лабораторной работе	7-8

3. Содержание оценочных средств текущего контроля

Оценочное средство 1:
Шаблон отчета по лабораторным работам прикреплен в файле.
Оценочное средство 2:
Тест. Примерные вопросы к тесту прикреплены к файлу.

4. Содержание оценочных средств промежуточной аттестации

Семестр 1:

Вид аттестационного испытания 1: Устное собеседование.
Форма проведения промежуточной аттестации: Экзамен.
Типовые задания: Вопросы к зачету с оценкой.

5. Методические материалы, определяющие процедуры оценивания знаний, умений, навыков и (или) опыта деятельности, характеризующие процесс формирования компетенций

Модуль состоит из набора разделов. Объем учебного раздела раскрывает отдельную (ые) тему(ы) модуля / этап прохождения практики. Модуль разбивается, как правило, на 2-4 раздела в семестр.

Раздел состоит из учебных элементов (дидактических единиц), сгруппированных по темам в рамках раздела. Объем учебного материала учебного элемента раскрывает отдельный вопрос темы. Путем набора соответствующих тем и учебных элементов формируется раздел, содержание которого соответствует запланированным результатам освоения ОП согласно учебному плану.

По каждому разделу устанавливается перечень обязательных видов работы студента, включающий: ответы на теоретические вопросы на семинаре; решение практических задач и выполнение заданий на практических занятиях; выполнение лабораторных работ; выполнение контрольных работ; написание рефератов; участие в коллоквиумах; тестирование по теме (группе тем); другие виды работ, определяемые преподавателем (в соответствии с установленными требованиями балльно-рейтинговой технологии).

Каждый раздел включает определенные формы контроля для оценки уровня усвоения учебного материала и определения рейтинговой оценки качества усвоения учебного материала.

Рейтинговая оценка знаний студентов определяется по 100-балльной шкале в каждом семестре и включает текущий, рубежный и итоговый контроль.

Накопленный рейтинг (фиксированная величина по окончании семестра) — это фактический рейтинг по всем освоенным к данному моменту разделам дисциплины, включая их текущий, рубежный и итоговый контроль, составляет N баллов (N – индивидуальная величина, зависящая от проделанной работы студента по дисциплине).

Проходной рейтинг (включает текущий контроль, рубежный контроль в семестре и промежуточную аттестацию) — это минимум баллов, набрав который студент будет считаться аттестованным по дисциплине, составляет 60 баллов в семестр по одной дисциплине.

Пороговый рейтинг (включает текущий контроль и рубежный контроль в семестре) — это минимальный фактический рейтинг семестрового контроля, набрав который, студент проходит на итоговый контроль, составляет 50% от суммы баллов, которые студент может набрать за текущий контроль и рубежный контроль в течение семестра.

Текущий контроль служит для получения первичной информации о ходе усвоения отдельных элементов содержания учебной дисциплины. Основное его назначение состоит в осуществлении контроля за всеми видами аудиторной и самостоятельной внеаудиторной деятельности студентов, результаты которого оцениваются в баллах.

Рубежный контроль (контрольные точки текущего контроля) проводится после изучения завершенной в смысловом и логическом плане части учебного материала (раздела, модуля). Этот вид контроля позволяет получить информацию о ходе усвоения некоторой совокупности содержательных элементов учебной дисциплины (раздела, модуля) и оценивается в баллах.

Промежуточный итоговый контроль (контрольные точки промежуточной аттестации) – курсовой проект, курсовая работа и экзамен, зачет, зачет с оценкой. Итоговый контроль по дисциплине в семестре предназначен для аттестации студента по учебной дисциплине: процедура установления соответствия уровня и качества подготовки студентов системе требований, зафиксированной в ФГОС ВО.

Распределение баллов рейтинговой оценки между видами контроля

Таблица 3

Номер семестра	Распределение баллов					Проходной рейтинг
	Текущий и рубежный контроль			Промежуточный итоговый контроль		
	Текущий контроль	Рубежный контроль	Пороговый рейтинг	Курсовая работа/курсовой проект	Зачет/зачет с оценкой/экзамен	
1	40	30	35	0	30	60

Перевод оценок 100-балльной шкалы в оценки промежуточной аттестации

Таблица 4

100-балльная шкала	85-100	75-84	60-74	0-59
5-балльная шкала	Отлично	Хорошо	Удовлетворительно	Неудовлетворительно
Бинарная шкала	Зачтено			Не зачтено

Распределение рейтинговых баллов по разделам модуля с указанием применяемых для их начисления оценочных средств представлено в Технологической карте БРТ.

Технологическая карта БРТ

Семестр 1

Раздел учебного модуля	Оценочные средства			Итого
	Отчёт по лабораторной работе	**Контрольная точка в форме тестирования**	**Экзамен**	
Раздел 1				
ЛР 1.1	5	0		5
ЛР 1.2	5	0		5
ЛР 1.3	5	0		5
ЛР 1.4	5	30		35
Итого по разделу 1	20	30		50
Раздел 2				
ЛР 2.5	5			5
ЛР 2.6	5			5
ЛР 2.7	5			5
ЛР 2.8	5			5
Итого по разделу 2	20			20
Промежуточная аттестация			30	30
Итого	40	30	30	100

Требования к отчету по практическому занятию дисциплины "Основы кибербезопасности"

Цель отчета:

Отчет по практическому занятию по дисциплине "Основы кибербезопасности" направлен на оценку степени понимания и применения студентами теоретических знаний в области комплексной системы защиты информации на предприятии. Отчет также демонстрирует умение анализировать и решать задачи, связанные с обеспечением безопасности информации.

Общие требования:

1. Отчет должен быть оформлен в электронном виде в формате Microsoft Word или PDF.

2. Отчет должен содержать титульный лист с указанием названия университета, факультета, кафедры, названия дисциплины, номера и названия практического занятия, ФИО студента, номера группы, учебного курса и даты выполнения отчета.

3. Отчет должен быть написан на русском языке с соблюдением правил грамматики и орфографии.

Структура отчета:

1. Введение:

- Краткое описание цели и задач практического занятия.

2. Основная часть:

- Описание предложенной задачи или сценария, связанного с комплексной системой защиты информации на предприятии.
- Применение теоретических знаний из дисциплины для решения задачи.
- Описание шагов и методов, использованных для решения задачи.
- Обоснование принятых решений и выбранных подходов.
- Анализ возможных рисков и уязвимостей, а также способов их устранения или минимизации.

3. Заключение:

- Сводная информация о результатах практического занятия.
- Оценка эффективности примененных мер и методов.
- Выводы, сделанные на основе выполненных задач и анализа результатов.

4. Список использованных источников:

- Перечень литературы, статей, интернет-ресурсов и других источников, использованных при подготовке отчета

Примечания:

- Отчет должен быть оформлен с использованием форматирования шрифтов, заголовков, списков и других элементов, чтобы обеспечить его читаемость и структурированность.

- В случае, если задача для практического занятия предоставляется преподавателем, следует строго следовать указаниям и требованиям, предоставленным для задачи.

- Оценка отчета будет учитывать как правильность решения задачи, так и грамотность изложения и оформления.

Срок сдачи отчета:

Срок сдачи отчета уточняется преподавателем в соответствии с графиком проведения практических занятий. Отчеты, сданные после установленного срока, могут быть оценены с сокращением баллов.

Оценка отчета:

Оценка отчета будет учитывать такие критерии, как правильность решения задачи, адекватность выбранных подходов, анализ рисков и уязвимостей, логичность изложения, использование источников и оформление отчета.

Дата утверждения требований: [Дата утверждения]

Перечень вопросов для промежуточной аттестации (зачет)

1. Что такое кибербезопасность и почему она важна в современном мире?

2. Объясните, что такое уязвимость в контексте информационной безопасности.

3. Какие типы киберугроз вы знаете? Приведите примеры каждого типа.

4. Что такое аутентификация и почему она важна для обеспечения безопасности систем?

5. Что такое многофакторная аутентификация? Какие факторы могут быть использованы при многофакторной аутентификации?

6. Объясните понятие "зловредное ПО" (вредоносное программное обеспечение). Какие виды зловредного ПО вы знаете?

7. Что такое фишинг? Какие меры можно предпринять для защиты от фишинговых атак?

8. Как работает атака "человек посередине" (Man-in-the-Middle)? Как можно защититься от такой атаки?

9. Что представляет собой атака DDoS? Какие методы защиты от DDoS-атак существуют?

10. Какие меры можно предпринять для обеспечения безопасности на рабочем месте, включая использование общедоступных Wi-Fi сетей?

11. Что такое шифрование данных? Какие методы шифрования вы знаете?

12. Какую роль играет бэкдор (backdoor) в кибербезопасности? Как они могут быть использованы злоумышленниками?

13. Что такое антивирусное программное обеспечение? Какие типы вредоносных программ оно может обнаруживать?

14. Какое значение имеет понятие "социальная инженерия" в контексте кибербезопасности?

15. Что такое VPN (виртуальная частная сеть)? Какие преимущества предоставляет использование VPN?

16. Какие методы аудита безопасности существуют и зачем они используются?

17. Что представляет собой "IoT" (Интернет вещей) и какие угрозы могут возникнуть в связи с его распространением?

18. Какие методы защиты паролей вы знаете? Какой пароль считается более надежным?

19. Что такое "фаервол" (firewall) и какую роль он выполняет в кибербезопасности?

20. Как можно обезопаситься от социальных сетей и предотвратить утечку личных данных?

ДИАГНОСТИЧЕСКАЯ РАБОТА ПО ОСНОВНОЙ ОБРАЗОВАТЕЛЬНОЙ ПРОГРАММЕ

09.03.01 Информатика и вычислительная техника

шифр и наименование направления подготовки/ специальности

Автоматизированные системы обработки информации и управления

наименование профиля/специализации

очная

форма обучения

2/104

курс/группа (ы)

Проверяемые компетенции:
1. ПК-1 Способен анализировать и разрабатывать требования к программному обеспечению
2. ПК-6 Способен осуществлять оценку соответствия требованиям существующих и проектируемых систем и сопровождать приемочные испытания и ввод в эксплуатацию

Номер задания	Содержание задания	Ключ к ответу	Наименование дисциплины (практики), формирующей данную компетенцию	Наименование темы РПД	Семестр
ПК-1 Способен анализировать и разрабатывать требования к программному обеспечению					
1.	Прочитайте текст вопроса и выберите один правильный ответ Какое из перечисленных свойств НЕ входит в триаду CIA (основные цели информационной безопасности)? 1. Доступность 2. Актуальность 3. Целостность 4. Конфиденциальность	2	Основы защиты информации	Основы классической криптографии	4
2.	Прочитайте текст вопроса и выберите правильный ответ: Укажите принцип, который лежит в основе современной криптографии. 1. Секретность алгоритма шифрования 2. Секретность длины ключа	3	Основы защиты информации	Основы криптографии	4

	3. Секретность только ключа при открытости алгоритма 4. Открытость и ключа, и алгоритма				
3.	Прочитайте текст вопроса и выберите два правильных ответа: Укажите алгоритмы, которые относятся к симметричным блочным шифрам. 1. AES 2. RSA 3. ГОСТ 28147-89 4. DSA 5. SHA-256	13	Основы защиты информации	Симметричные алгоритмы шифрования	4
4.	Прочитайте текст вопроса и выберите три правильных ответа: Укажите виды мер защиты информации, применяемые на практике. 1. Организационные 2. Правовые 3. Технические 4. Психологические 5. Финансовые	123	Основы защиты информации	Криптографические системы защиты информации	4
5.	Прочитайте текст вопроса и установите последовательность. Запишите соответствующую последовательность цифр слева направо. Установите правильную последовательность этапов создания электронной цифровой подписи. 1. Проверка подлинности ЭП получателем 2. Вычисление хеш-функции от документа 3. Передача документа получателю 4. Шифрование хеша закрытым ключом отправителя	2431	Основы защиты информации	Алгоритм цифровой подписи	4
6.	Прочитайте текст и установите соответствие. К каждой позиции, данной в левом столбце, подберите соответствующую позицию из правого столбца. Запишите выбранные цифры под соответствующими буквами. Тип алгоритма A. Симметричный алгоритм B. Асимметричный алгоритм C. Хеш-функция D. Электронная цифровая подпись 1. Использует пару ключей (открытый и закрытый) 2. Использует один ключ для шифрования и расшифрования 3. Односторонняя функция, устойчивая к коллизиям 4. Обеспечивает аутентичность и целостность сообщения	A-2 B-1 C-3 D-4	Основы защиты информации	Хэш-функции	4
7.	Прочитайте текст и дополните фразу: Основная задача хеш-функции при формировании электронной цифровой подписи заключается в вычислении _____ сообщения фиксированной длины.	хеш-образа (хеш-кода, дайджеста)	Основы защиты информации	Хэш-функции	4

ПК-6 Способен осуществлять оценку соответствия требованиям существующих и проектируемых систем и сопровождать приемочные испытания и ввод в эксплуатацию					
8.	Прочитайте текст вопроса и установите последовательность. Запишите соответствующую последовательность цифр слева направо. Установите последовательность этапов тестирования системы на проникновение. 1. Сбор информации и разведка 2. Получение доступа и эксплуатация 3. Сканирование и выявление уязвимостей 4. Анализ результатов и отчёт	1324	Основы защиты информации	Криптографические системы защиты информации	4
9.	Прочитайте текст и установите соответствие. К каждой позиции, данной в левом столбце, подберите соответствующую позицию из правого столбца. Запишите выбранные цифры под соответствующими буквами.Метод тестирования A. Статический анализ B. Динамическое тестирование C. Пенетрационное тестирование D. Фаззинг 1. Анализ исходного кода без запуска программы 2. Тестирование работающей системы 3. Активная имитация атаки на систему 4. Автоматическая подача случайных данных для поиска ошибок	A-1 B-2 C-3 D-4	Основы защиты информации	Криптографические системы защиты информации	4
10.	Прочитайте текст и дополните фразу: Наиболее эффективный способ проверки стойкости пароля в системе — это тестирование методом и словарной атаки.	перебора (brute-force)	Основы защиты информации	Основы криптографии	4