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

Кибербезопасность

УГСН	09.00.00 Информатика и вычислительная техника
Направление подготовки (специальность)	09.03.02 Информационные системы и технологии
Квалификация	*Бакалавр*
Форма обучения	*Очная*
Год начала подготовки	*2023*
Объем дисциплины, ч. / з.е. / недели	*108/3/2*
Образовательные технологии	*Традиционные*
Форма контроля (промежуточная аттестация)	*Экзамен*
Подразделение – разработчик	*Кафедра "Информационные технологии"*

Самара 2023

Кибербезопасность

Разработчик

Разработчик РПМ
Глушак Елена Владимировна
Руководитель подразделения
Колоденкова Анна Евгеньевна

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 Проектирует и разрабатывает информационные системы и хранилища данных с современным графическим интерфейсом и организацией сетевого взаимодействия	ПК-1.7 Определяет характеристики и анализирует качество информационных систем с помощью современных методик тестирования программного обеспечения	Знать: основные понятия в области кибербезопасности; основные угрозы, риски и уязвимости в сфере кибербезопасности Уметь: анализировать существующие угрозы, свойства информации как объекта защиты от киберугроз Владеть: реализовывать методы защиты информации и применять различные алгоритмы шифрования, организовывать сетевое взаимодействие с возможностью защиты информации

2. Место модуля в структуре образовательной программы

Модуль входит в Вариативную часть.

Входные требования:

Предшествующие осваиваемые модули: Этичный хакинг;

Последующие осваиваемые модули: Программирование Blockchain, Проектирование и разработка интерфейсов информационных систем, Методы и технологии машинного обучения, Распределенные базы данных.

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	*47*	*0*	*0*	*47*
Подготовка к экзамену	*10*	*0*	*0*	*10*
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.	Кибербезопасность: основные понятия и определения	2	2	0	4	8
4.	Классификация угроз	2	4	0	7	13
5.	Методы защиты информации с применением симметричных алгоритмов шифрования	2	4	0	8	14
6.	Методы защиты информации с применением асимметричных алгоритмов шифрования	2	6	0	8	16
7.	Методы защиты информации с применением методов основанных на разделении данных	2	6	0	8	16
8.	Математические модели шифра Виженера и численных методы его реализации	2	4	0	8	14
2.	Сетевые технологии и протоколы: основные понятия и определения	2	2	0	7	11
3.	Основные понятия и определения информационной безопасности	2	4	0	7	13
	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.	Кибербезопасность: основные понятия и определения	Кибербезопасность: основные понятия и определения	Основные понятия в области кибербезопасности; основные угрозы, риски и уязвимости в сфере кибербезопасности и критической информационной инфраструктуры	2	0
4.	Классификация угроз	Классификация угроз	Существующие угрозы, понятие информации и информатизации, свойства информации как объекта защиты от киберугроз, антивирусы и базовая защита электронного документооборота от не санкционированного доступа	2	0
5.	Методы защиты информации с применением симметричных алгоритмов шифрования	Методы защиты с применением симметричного шифрования	Принципы построения системы кибербезопасности, определение уязвимостей автоматизированных систем и выбор средств защиты, формирование требований к построению систем криптографической и стеганографической защиты, методы защиты с применением алгоритмов симметричного шифрования: 1. Шифры перестановки.	2	0
6.	Методы защиты информации с применением асимметричных алгоритмов шифрования	Методы защиты с применением ассимметричного шифрования	Общие требования к паролям асимметричного шифрования, основы стеганографии, защищенные каналы данных, облачные технологии	2	0
7.	Методы защиты информации с применением методов основанных на разделении данных	Методы защиты, основанные на разделении данных	Анализ основных методов защиты, основанных на разделении данных, криптографическая защита, технические средства обеспечения безопасности данных	2	0
8.	Математические модели шифра Виженера и численных методы его реализации	Математические модели шифра Виженера	Изучение математических моделей шифра Виженера и численных методов его реализации, криптоанализ шифра Виженера, метод Казиски	2	0
2.	Сетевые технологии и протоколы: основные понятия и определения	Понятия и определения сетевых технологий	Основные понятия и определения сетевых технологий, проблемы и их решения	2	0

№ ЛЗ	Наименование раздела	Тема лекции	Содержание лекции (перечень дидактических единиц: рассматриваемых подтем, вопросов)	Количество часов	Количество часов в электронной форме
3.	Основные понятия и определения информационной безопасности	Информационная безопасность	Основные понятия в сфере функциональной безопасности; - положения основных нормативных актов, регулирующих сферу безопасности информационной инфраструктуры; - архитектура основных подсистем обеспечения ИБ	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.	Кибербезопасность: основные понятия и определения	Анализ кибербезопасности	Основные понятия в области кибербезопасности; основные угрозы, риски и уязвимости в сфере кибербезопасности	2	0	*0*
5.	Классификация угроз	Существующие угрозы	Существующие угрозы, свойства информации как объекта защиты от киберугроз	2	0	*0*
6.	Классификация угроз	Существующие угрозы	Антивирусы и базовая защита электронного документооборота от не санкционированного доступа	2	0	*0*
7.	Методы защиты информации с применением симметричных алгоритмов шифрования	Методы защиты с применением симметричного шифрования	Принципы построения системы кибербезопасности, определение уязвимостей автоматизированных систем и выбор средств защиты, формирование требований к построению систем криптографической и стеганографической защиты	2	0	*0*
8.	Методы защиты информации с применением симметричных алгоритмов шифрования	Методы защиты с применением симметричного шифрования	1. Шифры перестановки. Анализ шифра простой перестановки. 2. Шифры замены. Анализ шифра замены. 3. Шифр XOR. Анализ шифра XOR	2	0	*0*
9.	Методы защиты информ	Методы защиты с применением	Общие требования к паролям асимметричного шифрования	2	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
	ации с применением асимметричных алгоритмов шифрования	ассимметричного шифрования				
10.	Методы защиты информации с применением асимметричных алгоритмов шифрования	Методы защиты с применением ассимметричного шифрования	Основы стеганографии	2	0	*0*
11.	Методы защиты информации с применением асимметричных алгоритмов шифрования	Методы защиты с применением ассимметричного шифрования	Защищенные каналы данных, облачные технологии	2	0	*0*
12.	Методы защиты информации с применением методов основанных на разделении данных	Методы защиты, основанные на разделении данных	Анализ основных методов защиты, основанных на разделении данных	2	0	*0*
13.	Методы защиты информации с применением методов основанных на разделении данных	Методы защиты, основанные на разделении данных	Криптографическая защита	2	0	*0*
14.	Методы защиты информации с применением методов основан	Методы защиты, основанные на разделении данных	Технические средства обеспечения безопасности данных	2	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
	ных на разделении данных					
15.	Математические модели шифра Виженера и численных методы его реализации	Математические модели шифра Виженера	Изучение математических моделей шифра Виженера и численных методов его реализации	2	0	*0*
16.	Математические модели шифра Виженера и численных методы его реализации	Математические модели шифра Виженера	Криптоанализ шифра Виженера, метод Казиски	2	0	*0*
2.	Сетевые технологии и протоколы: основные понятия и определения	Понятия и определения сетевых технологий	Анализ сетевых технологий	2	0	*0*
3.	Основные понятия и определения информационной безопасности	Информационная безопасность	Анализ информационной безопасности	2	0	*0*
4.	Основные понятия и определения информационной безопасности	Информационная безопасность	Архитектура основных подсистем обеспечения ИБ	2	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			
Кибербезопасность: основные понятия и определения	Подготовка к лабораторным работам	Изучение основных понятий в области кибербезопасности	2
Кибербезопасность: основные понятия и определения	Подготовка к экзамену	Основные понятия в области кибербезопасности; основные угрозы, риски и уязвимости в сфере кибербезопасности	2
Классификация угроз	Подготовка к лабораторным работам	Изучение и анализ существующих программ антивирусов и базовой защиты электронного документооборота от не санкционированного доступа	7
Методы защиты информации с применением симметричных алгоритмов шифрования	Подготовка к лабораторным работам	Изучение существующих шифров	8
Методы защиты информации с применением асимметричных алгоритмов шифрования	Подготовка к лабораторным работам	Изучение требований к паролям асимметричного шифрования	8
Методы защиты информации с применением методов основанных на разделении данных	Подготовка к экзамену	Технические средства обеспечения безопасности данных	8
Математические модели шифра Виженера и численных методы его реализации	Подготовка к лабораторным работам	Изучение математических моделей шифра Виженера и численных методов его реализации	8
Сетевые технологии и протоколы: основные понятия и определения	Подготовка к лабораторным работам	Изучение архитектуры основных подсистем обеспечения ИБ	7
Основные понятия и определения информационной безопасности	Подготовка к лабораторным работам	Анализ информационной безопасности, анализ ее возможностей	7
		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
1.	Ворожейкин, В.Н. Технические средства и методы защиты информации – дополнительные главы : Лабораторный практикум / В. Н. Ворожейкин; Самар.гос.техн.ун-т, Электронные системы и информационная безопасность .- 2-е изд..- Самара, 2019.- 336 с.	Электронная библиотека СамГТУ (ЭБС Политех)
2.	Кибербезопасность в условиях электронного банкинга; Прометей, 2020	ЭБС IPR Books
3.	Краковский, Ю.М. Информационная безопасность и защита информации : Учеб.пособие / Ю. М. Краковский.- М., МарТ, 2008.- 287 с.	Книжный фонд СамГТУ
4.	Основы кибербезопасности. Стандарты, концепции, методы и средства обеспечения; Техносфера, 2021	ЭБС IPR Books
5.	Информационная безопасность и защита информации; Самарский государственный архитектурно-строительный университет, ЭБС АСВ, 2014	ЭБС IPR Books
6.	Кибероружие и кибербезопасность. О сложных вещах простыми словами; Инфра-Инженерия, 2020	ЭБС IPR Books

7.	Прохорова, Ольга Витольдовна Информационная безопасность и защита информации : учеб. [для 2 курса специальности 230400.62 "Информ. системы и технологии"] [Текст] / Самар. гос. архитектур.-строит. ун-т (СГАСУ), Каф. приклад. математики и вычисл. техники.- Самара, СГАСУ, 2014.- 112 с.: ил.	Книжный фонд АСА СамГТУ

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.	*Scopus: база данных рефератов и цитирования [Электронный ресурс]. - Электрон. текстовые, граф., зв. дан., Сайт в сети Интернет*	*http://www.scopus.com*	*Ресурсы ограниченного доступа*
2.	*Библиотека компьютерной литературы [Электронный ресурс]. - Электрон. текстовые, граф., зв. дан., Сайт в сети Интернет*	*http://it.eup.ru/*	*Ресурсы открытого доступа*

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

Лекционные занятия проводятся в:
Корпус № 8/414 - Учебная аудитория.

Практические занятия не предусмотрены.

Самостоятельная работа проводятся в:
Корпус № 8/419 - Компьютерный класс
Корпус № 8/422 - Компьютерный класс.

Лабораторные занятия проводятся в:
Корпус № 8/422 - Компьютерный класс
Корпус № 8/419 - Компьютерный класс.

ПРИЛОЖЕНИЕ
Фонд оценочных средств

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

Настоящий Фонд оценочных средств (ФОС) по модулю Кибербезопасность 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	Устный опрос	Диалог преподавателя со студентом, цель которого – систематизация и уточнение имеющихся у студента знаний, проверка его индивидуальных возможностей усвоения материала.	8	Перечень вопросов для обсуждения
2	Отчёт по лабораторной работе	Оценка способности студента применить полученные ранее знания для проведения анализа, опыта, эксперимента и выполнения последующих расчетов, а также составления выводов.	16	Требования к содержанию и оформлению отчета
3	Контрольная точка в форме контрольной работы	Средство рубежного контроля остаточных знаний и умений, обычно состоящее из нескольких вопросов или заданий, которые студент должен решить, выполнить.	1	Пример варианта контрольной работы

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
Кибербезопасность: основные понятия и определения	ПК-1.7 Определяет характеристики и анализирует качество информационных систем с помощью современных методик тестирования программного обеспечения	Знать: основные понятия в области кибербезопасности; основные угрозы, риски и уязвимости в сфере кибербезопасности Уметь: анализировать существующие угрозы, свойства информации как объекта защиты от киберугроз Владеть: реализовывать методы защиты информации и применять различные алгоритмы шифрования, организовывать	Устный опрос	1

		сетевое взаимодействие с возможностью защиты информации		
Кибербезопасность: основные понятия и определения	ПК-1.7 Определяет характеристики и анализирует качество информационных систем с помощью современных методик тестирования программного обеспечения	Знать: основные понятия в области кибербезопасности; основные угрозы, риски и уязвимости в сфере кибербезопасности Уметь: анализировать существующие угрозы, свойства информации как объекта защиты от киберугроз Владеть: реализовывать методы защиты информации и применять различные алгоритмы шифрования, организовывать сетевое взаимодействие с возможностью защиты информации	Отчёт по лабораторной работе	1
Классификация угроз	ПК-1.7 Определяет характеристики и анализирует качество информационных систем с помощью современных методик тестирования программного обеспечения	Знать: основные понятия в области кибербезопасности; основные угрозы, риски и уязвимости в сфере кибербезопасности Уметь: анализировать существующие угрозы, свойства информации как объекта защиты от киберугроз Владеть: реализовывать методы защиты информации и применять различные алгоритмы шифрования, организовывать сетевое взаимодействие с возможностью защиты	Устный опрос	2

		информации		
Классификация угроз	ПК-1.7 Определяет характеристики и анализирует качество информационных систем с помощью современных методик тестирования программного обеспечения	Знать: основные понятия в области кибербезопасности; основные угрозы, риски и уязвимости в сфере кибербезопасности Уметь: анализировать существующие угрозы, свойства информации как объекта защиты от киберугроз Владеть: реализовывать методы защиты информации и применять различные алгоритмы шифрования, организовывать сетевое взаимодействие с возможностью защиты информации	Отчёт по лабораторной работе	2
Методы защиты информации с применением симметричных алгоритмов шифрования	ПК-1.7 Определяет характеристики и анализирует качество информационных систем с помощью современных методик тестирования программного обеспечения	Знать: основные понятия в области кибербезопасности; основные угрозы, риски и уязвимости в сфере кибербезопасности Уметь: анализировать существующие угрозы, свойства информации как объекта защиты от киберугроз Владеть: реализовывать методы защиты информации и применять различные алгоритмы шифрования, организовывать сетевое взаимодействие с возможностью защиты информации	Устный опрос	3
Методы защиты информации с применением	ПК-1.7 Определяет	Знать: основные	Отчёт по лабораторной работе	3

симметричных алгоритмов шифрования	характеристики и анализирует качество информационных систем с помощью современных методик тестирования программного обеспечения	понятия в области кибербезопасности; основные угрозы, риски и уязвимости в сфере кибербезопасности Уметь: анализировать существующие угрозы, свойства информации как объекта защиты от киберугроз Владеть: реализовывать методы защиты информации и применять различные алгоритмы шифрования, организовывать сетевое взаимодействие с возможностью защиты информации		
Методы защиты информации с применением асимметричных алгоритмов шифрования	ПК-1.7 Определяет характеристики и анализирует качество информационных систем с помощью современных методик тестирования программного обеспечения	Знать: основные понятия в области кибербезопасности; основные угрозы, риски и уязвимости в сфере кибербезопасности Уметь: анализировать существующие угрозы, свойства информации как объекта защиты от киберугроз Владеть: реализовывать методы защиты информации и применять различные алгоритмы шифрования, организовывать сетевое взаимодействие с возможностью защиты информации	Устный опрос	4
Методы защиты информации с применением асимметричных алгоритмов шифрования	ПК-1.7 Определяет характеристики и анализирует качество информационных систем с помощью современных методик тестирования	Знать: основные понятия в области кибербезопасности; основные угрозы, риски и уязвимости в сфере кибербезопасности	Отчёт по лабораторной работе	4

	программного обеспечения	Уметь: анализировать существующие угрозы, свойства информации как объекта защиты от киберугроз Владеть: реализовывать методы защиты информации и применять различные алгоритмы шифрования, организовывать сетевое взаимодействие с возможностью защиты информации		
Методы защиты информации с применением асимметричных алгоритмов шифрования	ПК-1.7 Определяет характеристики и анализирует качество информационных систем с помощью современных методик тестирования программного обеспечения	Знать: основные понятия в области кибербезопасности; основные угрозы, риски и уязвимости в сфере кибербезопасности Уметь: анализировать существующие угрозы, свойства информации как объекта защиты от киберугроз Владеть: реализовывать методы защиты информации и применять различные алгоритмы шифрования, организовывать сетевое взаимодействие с возможностью защиты информации	Контрольная точка в форме контрольной работы	4
Методы защиты информации с применением методов основанных на разделении данных	ПК-1.7 Определяет характеристики и анализирует качество информационных систем с помощью современных методик тестирования программного обеспечения	Знать: основные понятия в области кибербезопасности; основные угрозы, риски и уязвимости в сфере кибербезопасности Уметь: анализировать существующие угрозы, свойства информации как объекта защиты от	Устный опрос	5

		киберугроз Владеть: реализовывать методы защиты информации и применять различные алгоритмы шифрования, организовывать сетевое взаимодействие с возможностью защиты информации		
Методы защиты информации с применением методов основанных на разделении данных	ПК-1.7 Определяет характеристики и анализирует качество информационных систем с помощью современных методик тестирования программного обеспечения	Знать: основные понятия в области кибербезопасности; основные угрозы, риски и уязвимости в сфере кибербезопасности Уметь: анализировать существующие угрозы, свойства информации как объекта защиты от киберугроз Владеть: реализовывать методы защиты информации и применять различные алгоритмы шифрования, организовывать сетевое взаимодействие с возможностью защиты информации	Отчёт по лабораторной работе	5
Математические модели шифра Виженера и численных методы его реализации	ПК-1.7 Определяет характеристики и анализирует качество информационных систем с помощью современных методик тестирования программного обеспечения	Знать: основные понятия в области кибербезопасности; основные угрозы, риски и уязвимости в сфере кибербезопасности Уметь: анализировать существующие угрозы, свойства информации как объекта защиты от киберугроз Владеть: реализовывать методы защиты информации и применять	Устный опрос	6

		различные алгоритмы шифрования, организовывать сетевое взаимодействие с возможностью защиты информации		
Математические модели шифра Виженера и численных методы его реализации	ПК-1.7 Определяет характеристики и анализирует качество информационных систем с помощью современных методик тестирования программного обеспечения	Знать: основные понятия в области кибербезопасности; основные угрозы, риски и уязвимости в сфере кибербезопасности Уметь: анализировать существующие угрозы, свойства информации как объекта защиты от киберугроз Владеть: реализовывать методы защиты информации и применять различные алгоритмы шифрования, организовывать сетевое взаимодействие с возможностью защиты информации	Отчёт по лабораторной работе	6
Сетевые технологии и протоколы: основные понятия и определения	ПК-1.7 Определяет характеристики и анализирует качество информационных систем с помощью современных методик тестирования программного обеспечения	Знать: основные понятия в области кибербезопасности; основные угрозы, риски и уязвимости в сфере кибербезопасности Уметь: анализировать существующие угрозы, свойства информации как объекта защиты от киберугроз Владеть: реализовывать методы защиты информации и применять различные алгоритмы шифрования, организовывать сетевое взаимодействие с	Устный опрос	7

		возможностью защиты информации		
Сетевые технологии и протоколы: основные понятия и определения	ПК-1.7 Определяет характеристики и анализирует качество информационных систем с помощью современных методик тестирования программного обеспечения	Знать: основные понятия в области кибербезопасности; основные угрозы, риски и уязвимости в сфере кибербезопасности Уметь: анализировать существующие угрозы, свойства информации как объекта защиты от киберугроз Владеть: реализовывать методы защиты информации и применять различные алгоритмы шифрования, организовывать сетевое взаимодействие с возможностью защиты информации	Отчёт по лабораторной работе	7
Основные понятия и определения информационной безопасности	ПК-1.7 Определяет характеристики и анализирует качество информационных систем с помощью современных методик тестирования программного обеспечения	Знать: основные понятия в области кибербезопасности; основные угрозы, риски и уязвимости в сфере кибербезопасности Уметь: анализировать существующие угрозы, свойства информации как объекта защиты от киберугроз Владеть: реализовывать методы защиты информации и применять различные алгоритмы шифрования, организовывать сетевое взаимодействие с возможностью защиты информации	Устный опрос	8

Основные понятия и определения информационной безопасности	ПК-1.7 Определяет характеристики и анализирует качество информационных систем с помощью современных методик тестирования программного обеспечения	Знать: основные понятия в области кибербезопасности; основные угрозы, риски и уязвимости в сфере кибербезопасности Уметь: анализировать существующие угрозы, свойства информации как объекта защиты от киберугроз Владеть: реализовывать методы защиты информации и применять различные алгоритмы шифрования, организовывать сетевое взаимодействие с возможностью защиты информации	Отчёт по лабораторной работе	8

3. Содержание оценочных средств текущего контроля

Оценочное средство 1:
Перечень вопросов, на основании которых происходит устный вопрос студентов
Оценочное средство 2:
Перечень вопросов, на основании которых происходит отчет студентов по лабораторным работам
Оценочное средство 3:
Перечень вопросов, на основании которых проводится контрольная работа

4. Содержание оценочных средств промежуточной аттестации

Формат контроля промежуточной аттестации: *Устное собеседование.*
Форма проведения промежуточной аттестации: .
Типовые задания: Типовое задание включает в себя два вопроса: теоретический и практический.

5. Методические материалы, определяющие процедуры оценивания знаний, умений, навыков и (или) опыта деятельности, характеризующие процесс формирования компетенций *(данный раздел находится в разработки в части БРТ)*

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

Раздел состоит из учебных элементов (дидактических единиц). Объем учебного материала учебного элемента раскрывает отдельный вопрос темы или тему дисциплины (если раздел содержит несколько тем). Путем набора соответствующих учебных элементов формируется раздел, содержание которого соответствует запланированным результатам освоения ОП согласно учебному плану.

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

Каждый раздел завершается определенной (ыми) формой (ами) 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.

Распределение баллов рейтинговой оценки между видами контроля

Таблица 3

Форма промежуточной аттестации	Количество баллов			
	Текущий контроль	Рубежный контроль	Итоговый контроль	Сумма баллов
Экзамен	0	0	40	40

Перевод оценок 100-балльной шкалы в оценки промежуточной аттестации

Таблица 4

100-балльная шкала	85-100	70-84	50-69	0-49
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.

Раздел УМ	Оценочные средства				Итого
	Отчёт по лабораторной работе	**Контрольная точка в форме контрольной работы**	**Устный опрос**	**Экзамен**	
Раздел 1					
ЛЗ 1.1			1		1
ЛР 1.1	1				1
Итого по разделу 1	1		1		2
Раздел 2					
ЛЗ 2.1			1		1
ЛР 2.1	1				1
Итого по разделу 2	1		1		2
Раздел 3					
ЛЗ 3.1			1		1
ЛР 3.1	1				1
Итого по разделу 3	1		1		2
Раздел 4					
ЛЗ 4.1			1		1
ЛР 4.1	2				2
ЛР 4.2		0			0
ЛР 4.3	1				1
ЛР 4.4		30			30
Итого по разделу 4	3	30	1		34
Раздел 5					
ЛЗ 5.1			1		1
ЛР 5.1	2				2
Итого по разделу 5	2		1		3
Раздел 6					
ЛЗ 6.1			1		1
ЛР 6.1	2				2
Итого по разделу 6	2		1		3
Раздел 7					
ЛЗ 7.1			1		1
ЛР 7.1	1				1
Итого по разделу 7	1		1		2
Раздел 8					
ЛЗ 8.1			1		1
ЛР 8.1	1				1
Итого по разделу 8	1		1		2
Промежуточная аттестация				40	40
Итого	12	30	8	40	90

Оценочные средства (ОС)

Дисциплина: *Кибербезопасность*

Наименование категории (группы) компетенций	Код и наименование компетенции	Код и наименование индикатора достижения компетенции	Результаты обучения (знать, уметь, владеть, соотнесенные с индикаторами достижения компетенции)
Не предусмотрено	ПК-1 Проектирует и разрабатывает информационные системы и хранилища данных с современным графическим интерфейсом и организацией сетевого взаимодействия	Не предусмотрено	**Знать:** основные понятия в области кибербезопасности; основные угрозы, риски и уязвимости в сфере кибербезопасности **Уметь:** анализировать существующие угрозы, свойства информации как объекта защиты от киберугроз **Владеть:** реализовывать методы защиты информации и применять различные алгоритмы шифрования, организовывать сетевое взаимодействие с возможностью защиты информации

Код индикатора достижения компетенции	Результаты обучения	Оценочные средства	Текущий контроль успеваемости	Промежуточная аттестация
Кибербезопасность: основные понятия и определения				
ПК-1 Проектирует и разрабатывает информационные системы и хранилища данных с современным графическим интерфейсом и организацией сетевого взаимодействия	**Знать:** основные понятия в области кибербезопасности; **Уметь:** анализировать существующие угрозы, **Владеть:** методами и средствами технической защиты информации	Лабораторные работы	устный опрос на лабораторных работах	Самостоятельная работа
Сетевые технологии и протоколы: основные понятия и определения				
ПК-1 Проектирует и разрабатывает	**Знать:** сетевые технологии и протоколы;	Лабораторные работы	устный опрос на лабораторных работах	Самостоятельная работа

информационные системы и хранилища данных с современным графическим интерфейсом и организацией сетевого взаимодействия	**Уметь:** оценивать качество готового программного обеспечения, **Владеть:** методами расчета и инструментального контроля показателей технической защиты информации			
Классификация угроз				
ПК-1 Проектирует и разрабатывает информационные системы и хранилища данных с современным графическим интерфейсом и организацией сетевого взаимодействия	**Знать:** существующие угрозы; **Уметь:** использовать программные пакеты для обеспечения защищенной системы, **Владеть:** современными средствами защиты информации	Лабораторные работы	устный опрос на лабораторных работах	Самостоятельная работа
Методы защиты информации с применением симметричных алгоритмов шифрования				
ПК-1 Проектирует и разрабатывает информационные системы и хранилища данных с современным графическим интерфейсом и организацией сетевого взаимодействия	**Знать:** методы защиты информации; **Уметь:** использовать методы защиты информации, **Владеть:** современными системами компьютерной безопасности	Лабораторные работы	устный опрос на лабораторных работах	Самостоятельная работа
Методы защиты информации с применением асимметричных алгоритмов шифрования				
ПК-1 Проектирует и разрабатывает информационные системы и хранилища данных с современным графическим интерфейсом и организацией сетевого взаимодействия	**Знать:** методы защиты информации; **Уметь:** использовать методы защиты информации, **Владеть:** современными методами шифрования данных	Лабораторные работы	устный опрос на лабораторных работах	Самостоятельная работа
Методы защиты информации с применением методов основанных на разделении данных				
ПК-1	**Знать:**	Лабораторные	устный опрос на	Самостоятельная

Проектирует и разрабатывает информационные системы и хранилища данных с современным графическим интерфейсом и организацией сетевого взаимодействия	криптоанализ, современное состояние систем защиты; **Уметь:** использовать методы защиты информации на основе разделения данных, **Владеть:** современными путями решения проблемы информационной безопасности	работы	лабораторных работах	работа
Математические модели шифра Виженера и численных методы его реализации				
ПК-1 Проектирует и разрабатывает информационные системы и хранилища данных с современным графическим интерфейсом и организацией сетевого взаимодействия	**Знать:** основные модели шифров; **Уметь:** анализировать существующие решения проблем при шифровании данных, **Владеть:** методами и средствами технической защиты информации	Лабораторные работы	устный опрос на лабораторных работах	Самостоятельная работа
Основные понятия и определения информационной безопасности				
ПК-1 Проектирует и разрабатывает информационные системы и хранилища данных с современным графическим интерфейсом и организацией сетевого взаимодействия	**Знать:** основные понятия в области информационной безопасности; **Уметь:** анализировать существующие угрозы, **Владеть:** способами снижения угроз	Лабораторные работы	устный опрос на лабораторных работах	Самостоятельная работа

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

Формы текущего контроля успеваемости

Оценочное средство 1.
Устный опрос.

Раздел 1

1. Виды и характеристика способов информационной защиты на синтаксическом уровне.
2. Признаковая информация и формы ее защиты.
3. Виды кодирования информации.
4. Способы сжатия и декомпрессии компьютерной информации.
5. Характеристика информации как объекта собственности.
6. Общая характеристика информационных угроз.
7. Угрозы конфиденциальности, целостности и доступности.
8. Субъекты (источники и носители) информационных угроз.
9. Информационные нарушители и их классификация
10. Угрозы информации, связанные с человеческим фактором.
11. Пользователи как источники информационных угроз
12. «Внешние» нарушители информационной безопасности

Раздел 2

1. Основные федеральные законы в области защиты информации.
2. Технология двухфакторной аутентификации.
3. Идентификация в вычислительной системе.
4. Циклические коды.
5. Недостатки систем хеширования.
6. Способы защиты информации.
7. Стратегии защиты информации.
8. Периметр охраняемой территории.
9. «Абсолютная» система защиты.
10. Защита от утечки информации по техническим каналам. Термины и определения. Каналы утечки.
11. Основные способы защиты информации от утечки по техническим каналам.
12. Основные принципы защиты информации от электронных средств негласного подслушивания.
13. Общие принципы защиты компьютерной информации и ЭВМ от вредоносных программ.
14. Общая характеристика систем управления доступом.

Раздел 3

1. Модель абсолютной защиты для сложной информационной системы.
2. Стратегии информационной защиты.
3. Активные и пассивные способы обнаружения информационных угроз.
4. Стратегия пассивной защиты
5. Стратегия маскировки, имитации и дезинформации
6. Стратегия ликвидации источников и носителей информационных угроз
7. Сущность энергетического скрытия информации
8. Информационное скрытие на логическом и синтаксическом уровнях

9. Модель канала связи.
10. Угрозы информации в каналах связи
11. Методы защиты информации в каналах связи.
12. Виды и способы сокрытия источников и получателей сообщений в открытых информационных сетях.
13. Характеристика, этапы и демаскирующие признаки удаленного доступа к сетевой ЭВМ.
14. Модель комплексной защиты информации и ее элементы.
15. Общая характеристика нормативно-правовой защиты информации.
16. Защищаемая законом информация. Особенности правовой защиты информации ограниченного доступа.

Раздел 4

1. Информация, сообщения, информационные процессы как объекты информационной безопасности.
2. Понятие угрозы безопасности информации
3. Обзор защищаемых объектов и систем.
4. Понятие «угроза информации». Понятие «риска информационной безопасности».
5. Примеры преступлений в сфере информации и информационных технологий.
6. Сущность функционирования системы защиты информации.
7. Защита человека от опасной информации и от неинформированности в области информационной безопасности.
8. Целостность, доступность и конфиденциальность информации.
9. Классификация информации по видам тайны и степеням конфиденциальности.
10. Понятия государственной тайны и конфиденциальной информации.
11. Жизненные циклы конфиденциальной информации в процессе ее создания, обработки, передачи.
12. Цели и задачи защиты информации.
13. Основные понятия в области защиты информации.
14. Элементы процесса менеджмента ИБ.
15. Модель интеграции информационной безопасности в основную деятельность организации. 16. Понятие Политики безопасности.

Раздел 5

1. Чем шифрование отличается от кодирования?
2. Должен ли быть секретным алгоритм шифрования?
3. Должен ли быть секретным ключ шифра при симметричном шифровании?
4. Кто может знать алгоритм шифрования?
5. Кто должен знать ключ шифра?
6. Опишите как получается матрица Виженера.
7. Опишите методику шифрования текста шифром Виженера.
8. Опишите методику шифрования с закрытым ключом.
9. Опишите логическую операцию XOR.
10. В чем заключается алгоритм RSA?
11. Для чего и почему используют комбинированные криптоалгоритмы?
12. Поясните концепцию разбиения данных. Приведите пример.
13. Поясните концепцию порогового разделения данных. Приведите пример.
14. Поясните преимущества использование системы остаточных классов для разделения секрета.
15. Каким образом информация из системы остаточных классов переводится в десятичную систему счисления с применением обобщенной полиадической системы счисления.

Раздел 6

1. Что делать, если размер ключа меньше размера текста?
2. В чем заключается идея шифра простой замены?
3. Алфавиты открытого текста и шифртекста совпадают или отличаются?
4. Как соотносятся частоты появления открытого текста и шифротекста?
5. Сколько уникальных вариантов ключа можно получить для заданного размера блока?
6. Опишите методику нахождения длинны ключевого слова.
7. Опишите методику нахождения ключевого слова если известна его длинна.
8. Механизм работы шифрования на основе XOR
9. Насколько надежен рассмотренный алгоритм шифрования на основе XOR?
10. В чем заключаются достоинства и недостатки асимметричных алгоритмов?
11. В чем заключаются достоинства и недостатки симметричных алгоритмов?
12. Расскажите принцип порогового разделения данных с применением схемы Шамира.
13. Расскажите принцип порогового разделения данных с применением схемы Блэкли.
14. Расскажите принцип порогового разделения данных с применением схемы Миньотта.
15. Расскажите принцип порогового разделения данных с применением схемы Асмута-Блума.

Раздел 7

1. Что такое компьютерный вирус?
2. Назначение компьютерного вируса?
3. Типы вирусов.
4. Программные средства защиты – антивирусные программы (характеристика).
5. Безопасность программно-технических средств и информационных ресурсов (характеристика). 6. Программная защита от несанкционированных воздействий.
7. Криптография, криптографическая защита от несанкционированных воздействий (характеристика).
8. Что такое электронная подпись?
9. Физическая и техническая защита от несанкционированных воздействий (характеристика).
10.Воздействия на здания, помещения, личную безопасность пользователя и обслуживающий персонал.
11.Технические возможности и мероприятия по обеспечению сохранности людей, зданий, помещений, программно-технических средств и информации (характеристика).
12. Охрана объектов с целью ограничения свободного доступа, смарткарты и др. (характеристика)

Раздел 8

1. Опишите как получается матрица Виженера.
2. Опишите методику шифрования текста шифром Виженера.
3. Опишите методику шифрования с закрытым ключом.
4. Опишите логическую операцию XOR.
5. В чем заключается алгоритм RSA?
6. Поясните концепцию порогового разделения данных. Приведите пример.
7. Поясните преимущества использование системы остаточных классов для разделения секрета.
8. Каким образом информация из системы остаточных классов переводится в десятичную систему счисления с применением обобщенной полиадической системы счисления.
9. Вредоносные программы, их виды.
10. История компьютерных вирусов и современность.
11. Государственное регулирование информационной безопасности.
12. Электронная почта и ее защита.

Оценочное средство 2.
КОМПЛЕКТ ЗАДАНИЙ ДЛЯ ВЫПОЛНЕНИЯ САМОСТОЯТЕЛЬНОЙ РАБОТЫ

Способ организации самостоятельной работы: подготовка презентации на 12-15 слайдов с устным докладом по заданной тематике; разработка приложений по заданию преподавателя.

Темы с/р:
1. Проблема безопасности в условиях цифрового мира
2. Основные службы безопасности в информационных системах
3. Требования к реализации служб безопасности в составе разрабатываемого программного обеспечения
4. Стандарты безопасности
5. Типовые архитектурные решения безопасности
6. Угрозы кибербезопасности предприятия (организации) и способы борьбы с ними
7. Современные средства защиты информации
8. Современные системы компьютерной безопасности
9. Современные средства противодействия экономическому шпионажу
10. Современные криптографические системы.
11. Криптоанализ, современное состояние
12. Правовые основы защиты информации
13. Технические аспекты обеспечения защиты информации
14. Атаки на систему безопасности и современные методы защиты
15. Современные пути решения проблемы кибербезопасности РФ

При оценке самостоятельной работы студента учитываются:
- качество выполненной работы;
- логика изложения материала;
- полнота изучения темы исследования;
- правильность ответа на вопросы по теме;
- умение увязывать теоретические и практические аспекты вопроса;
- культура устной речи студента.

Оценочное средство 3.
Задания к контрольной работе.

Цель контрольной работы – закрепление и проверка знаний, полученных студентами заочной формы обучения в процессе самостоятельного изучения учебного материала.

Требования к содержанию и оформлению контрольной работы

Задание 1
1. Номер варианта контрольной работы определяется по последней цифре номера зачетной книжки (или по последней цифре порядкового номера Ф.И.О. студента в списке журнала группы, если он взят за основу при определении варианта); цифра «10» означает вариант № 10.
Распределение теоретических вопросов по вариантам приведено в таблице 1.

Таблица 1 – Распределение теоретических вопросов по вариантам

№ варианта	Номера вопросов				
1	1	11	21	31	41
2	2	12	22	32	42
3	3	13	23	33	43
4	4	14	24	34	44
5	5	15	25	35	45
6	6	16	26	36	46
7	7	17	27	37	47
8	8	18	28	38	48
9	9	19	29	39	49
10	10	20	30	40	50

Теоретические вопросы к контрольной работе

1. Что такое кибербезопасность? Информационная безопасность? Какие компоненты входят в информационную безопасность? Назовите пять этапов процесса информационной безопасности.
2. Почему безопасность – это процесс, а не конечный продукт?
3. Почему физическая защита не может гарантировать безопасность?
4. Выделите два основных типа межсетевых экранов. От какого нападения защищают межсетевые экраны?
5. Назовите основные категории атак. Всегда ли атака модификации включает в себя атаку доступа?
6. Назовите основные категории атак. К какому типу атак особенно уязвимы беспроводные сети?
7. Что определяет политика безопасности? Почему в политику безопасности включают отказы от защиты?
8. Угрозы и их составляющие. Может ли угроза иметь более одной цели? Назовите четыре цели для угроз.
9. Что определяет политика безопасности? Назовите четыре необходимых политики безопасности.
10. Назовите основные категории атак. Каковы три вида атак на схему шифрования?
11. Назовите три типа аутентификационных факторов. Почему двухфакторная аутентификация сильнее, чем однофакторная?
12. Зачем нужен аудит? На какие три службы безопасности должен опираться аудит?
13. Что такое уязвимость? Основные виды уязвимостей и их отличия. Приведите несколько рекомендаций по устранению уязвимостей.
14. Назовите две составляющих риска. Каков уровень риска при отсутствии угроз?
15. Назовите ключевые концепции стандарта ISO, в котором говорится об информационной безопасности.
16. Может ли шифрование полностью защитить данные, передаваемые через VPN.
17. Какие механизмы аутентификации лучше всего использовать для пользовательской VPN?
18. Что подразумевается под пассивными ответными действиями? Что подразумевается под активными ответными действиями?
19. Каков приблизительный радиус действия беспроводной сети стандарта 802.11x на открытой местности и в помещении? Почему аутентификация 802.1X сама по себе рассматривается как уязвимость в системе?

20. К какому типу сетей следует относить WLAN? Какую периодическую оценку необходимо проводить при работе с WLAN?
21. Является ли шифр Вермана подстановочным? Он моно- полиалфавитный? В чем заключается различие между шифром Вермана и одноразовым блокнотом?
22. Почему алгоритм AES считается очень эффективным? Как реализовать умножение в конечном поле F_{2^8} в алгоритме AES?
23. Почему в наборе параметров открытого ключа (e, N) криптосистемы RSA показатель степени e должен быть взаимно простым с числом $\phi(N)$?
24. Опишите атаки CPA, CCA и CCA2. Чем они отличаются?
25. Почему любой алгоритм шифрования в криптосистемах с открытым ключом (даже учебный) должен быть устойчивым к атаке CPA?
26. Что такое услуги оракула? Необходимы ли атакующему услуги оракула для расшифровки сообщений в криптосистеме с открытым ключом?
27. При каких условиях алгоритм шифрования RSA обладает свойством битовой стойкости?
28. Что обеспечивает стойкость алгоритмов, использующих генератор псевдослучайных чисел Блюма–Блюма–Шаба?
29. Проанализируйте фатальную уязвимость схемы Рабина для активных атак. Почему нестрогая стойкость учебных схем цифровых подписей непригодна для практического применения?
30. Является ли зашифрованный текст, созданный алгоритмом RSA–OAEP, корректным кодом MDC? Если является обоснуйте свой ответ.
31. Перечислите, какие виды угроз информационной безопасности в РФ существуют?
32. Перечислите внешние и внутренние источники угроз? В чем они отличаются?
33. Назовите основные задачи по обеспечению информационной безопасности в РФ?
34. Какие методы обеспечения информационной безопасности РФ существуют? В чем их отличия?
35. Перечислите сферы общественной жизни, которые затрагивают особенности обеспечения информационной безопасности РФ? В чем их особенности?
36. Какие существуют основные направления международного сотрудничества РФ? Чем они отличаются?
37. Назовите основные принципы государственной политики обеспечения информационной безопасности РФ? В чем отличия каждого из них?
38. Назовите первоочередные мероприятия по реализации государственной политики обеспечения информационной безопасности РФ? Какие они имеют отличия?
39. Какие основные функции обеспечения информационной безопасности РФ? Их особенности?
40. Основные элементы организационной основы системы обеспечения информационной безопасности РФ? Для чего они предназначены?
41. Какие виды деятельности в структуре правового обеспечения информационной безопасности вы знаете? В чем они отличаются?
42. Назовите составляющие, входящие в состав нормативного правового обеспечения информационной безопасности РФ? Дайте им полное описание?
43. Какие существуют принципы нормативного правового обеспечения информационной безопасности? Дайте им описание?
44. Назовите направления противоправных, злоумышленных действий на сетевой среде с целью использования их результатов для проведения террористических актов? Дайте им объяснения?
45. Назовите набор потенциальных сценариев террористических действий с использованием сетевой среды (Интернет) в самой общей постановке, в качестве взаимодействующих факторов, характеризующих «типовой профиль»? Дайте определения?

46. Назовите меры, которые будут способны противостоять угрозе конфиденциальности? Объясните их?
47. Чем отличается вирус от трояна?
48. Чем отличается SQL – инъекция от php – инклуда?
49. Объясните значение VBR–руткит?
50. Перечислите виды хешей, которые вы знаете (не менее 5)?

Задание 2

Рассмотреть антивирусные программы, подготовить доклад и иллюстрирующую его презентацию (MS PowerPoint, Impress) на 10–15 слайдов.

В презентации должно быть отражено:

- описание фирмы, выпустившей антивирусный продукт;
- немного истории появления (создания);
- описание антивирусной программы;
- список достоинств и недостатков антивирусной программы;

Презентация прилагается к контрольной работе на электронном носителе, доклад приводится в тексте контрольной работы.

Таблица 2 – Распределение антивирусных программ по вариантам

№ варианта	Название антивирусной программы
1	Avast! Free Antivirus
2	Kaspersky Antivirus
3	ESET Nod32
4	Trend Micro (PC–Cillin)
5	F–Secure Anti–Virus
6	McAfee VirusScan
7	Norton AntiVirus
8	AVG Internet Security
9	CA Antivirus
10	Norman Virus Control

Задание 3

Разработать программный код, выполняющий шифрование методом в соответствии с номером варианта. Файл с программой прилагается на электронном носителе, в тексте контрольной работе приводится блок–схема, листинг и скриншоты результатов работы программы.

1. Метод Цезаря со сдвигом на **3**.
2. Метод Гронсфельда с параметром **2178**.
3. Метод Вижинера с параметром **CODE.**
4. Метод Цезаря со сдвигом на **6**.
5. Метод Цезаря со сдвигом на **5**.
6. Метод Цезаря со сдвигом на **10**.
7. Метод Гронсфельда с параметром **2356**.
8. Метод Гронсфельда с параметром **15**.

9. Метод Вижинера с параметром **KEY.**
10. Метод Вижинера с параметром **INFO.**

Студент должен выполнить одно задание по выбору преподавателя. Задание считается выполненным (оценка «зачтено»), если результат его выполнения удовлетворяет требованиям, сформулированным преподавателем.

Оценочное средство 4.
Вопросы для подготовки к экзамену:
1. Понятие "информационная безопасность" и ее задачи
2. Составляющие информационной безопасности
3. Понятие защиты информации и ее задачи
4. Методы защиты препятствие;
5. Методы защиты управление доступом;
6. Методы защиты механизмы шифрования;
7. Методы защиты противодействие атакам вредоносных программ;
8. Методы защиты регламентация;
9. Методы защиты принуждение; 1
0. Методы защиты побуждение.
11. Информационная безопасность
12. Понятие кибербезопасности
13. Компьютерная безопасность
14. Компьютерные преступления
15. Понятие информационных угроз
16. Вредоносное программное обеспечение
17. Понятие киберпреступности
18. Классификация киберпреступности
19. Мошенничество и отмывание денег
20. Киберпреступность и терроризм
21. Хакеры
22. Спам
23. Киберпреступность и Интернет
24. Кибератаки
25. Кибератаки и их типы
26. Похищение паролей
27. Стадии Кибератаки
28. Защита от киберпреступности
29. Шифрование данных
30. Симметричное шифрование
31. Асимметричное шифрование или шифрование открытым ключом
32. ЭЦП
33. Защита документов MS Word
34. Защита документов MS Excel
35. Архивирование файлов Windows и их защита
36. Вирусы и методы борьбы с ними.
37. Антивирусные программы и пакеты.

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

Кафедра ИТ

ЭКЗАМЕНАЦИОННЫЙ БИЛЕТ №1

по дисциплине (модулю) *Кибербезопасность*

Код направления подготовки (специальности): 09.03.02 Институт АИТ Семестр 5

1. Классификация киберпреступности
2. Шифрование данных

Составил: *Глушак Е.В.* *10.05.2023*

Утверждаю: Заведующий кафедрой Колоденкова А.Е. *10.05.2023*

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

Кафедра ИТ

ЭКЗАМЕНАЦИОННЫЙ БИЛЕТ №2

по дисциплине (модулю) *Кибербезопасность*

Код направления подготовки (специальности): 09.03.02 Институт АИТ Семестр 5

1. Защита документов MS Word
2. Асимметричное шифрование или шифрование открытым ключом

Составил: *Глушак Е.В.* *10.05.2023*

Утверждаю: Заведующий кафедрой Колоденкова А.Е. *10.05.2023*

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

Кафедра ИТ

ЭКЗАМЕНАЦИОННЫЙ БИЛЕТ №3

по дисциплине (модулю) *Кибербезопасность*

Код направления подготовки (специальности): 09.03.02 Институт АИТ Семестр 5

1. Киберпреступность и Интернет
2. Стадии Кибератаки

Составил: *Глушак Е.В.* *10.05.2023*

Утверждаю: Заведующий кафедрой Колоденкова А.Е. *10.05.2023*

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

Кафедра ИТ

ЭКЗАМЕНАЦИОННЫЙ БИЛЕТ №4

по дисциплине (модулю) *Кибербезопасность*

Код направления подготовки (специальности): 09.03.02 Институт АИТ Семестр 5

1. Вредоносное программное обеспечение
2. Понятие киберпреступности

Составил: *Глушак Е.В.* *10.05.2023*

Утверждаю: Заведующий кафедрой Колоденкова А.Е. *10.05.2023*

Экзамен принимается в устной форме. Билет содержит два вопроса. На подготовку к ответу отводится 1 час.

Критерии оценивания на экзамене:
- **оценка «отлично»** выставляется студенту, если он глубоко и прочно усвоил программный материал, исчерпывающе, последовательно, четко и логически стройно его излагает, умеет тесно увязывать теорию с практикой, свободно справляется с задачами, вопросами и друг ими видами применения знаний, причём не затрудняется с ответом при видоизменении заданий, использует в ответе материал монографической литературы, правильно обосновывает принятое решение, владеет разносторонними навыками и приёмами выполнения практических задач. Элементы компетенций сформированы на высоком уровне;

- **оценка «хорошо»** выставляется студенту, если он твердо знает материал, грамотно и по существу излагает его, не допуская существенных неточностей в ответе на вопрос, правильно применяет теоретические положения при решении практических вопросов и задач, владеет необходимыми навыками и приемами их выполнения. Элементы компетенций в основном сформированы на среднем, но достаточно высоком уровне;

- **оценка «удовлетворительно»** выставляется студенту, если он имеет знания только основного материала, но не усвоил его деталей, допускает неточности, недостаточно правильные формулировки, нарушения логической последовательности в изложении программного материала, испытывает затруднения при выполнении практических работ. Элементы компетенций сформированы на достаточном, но минимальном пороговом уровне;

- **оценка «неудовлетворительно»** выставляется студенту, который не знает значительной части программного материала, допускает существенные ошибки, неуверенно, с большими затруднениями выполняет практические работы. Элементы компетенций не сформированы.

Оценочное средство 5
Тестирование

Вопрос 1:
Кто является основным ответственным за определение уровня классификации информации?
Варианты ответа:

1. Руководитель среднего звена
2. Высшее руководство
3. Владелец
4. Пользователь

Вопрос 2:
Какая категория является наиболее рискованной для компании с точки зрения вероятного мошенничества и нарушения безопасности?
Варианты ответа:

1. Сотрудники
2. Хакеры
3. Атакующие
4. Контрагенты (лица, работающие по договору)

Вопрос 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?
Варианты ответа:

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

Вопрос 4:
Что самое главное должно продумать руководство при классификации данных?
Варианты ответа:

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

Вопрос 5:
Кто в конечном счете несет ответственность за гарантии того, что данные классифицированы и защищены?
Варианты ответа:

1. Владельцы данных
2. Пользователи
3. Администраторы
4. Руководство

Вопрос 6:
Что такое процедура?
Варианты ответа:

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

Вопрос 7:
Какой фактор наиболее важен для того, чтобы быть уверенным в успешном обеспечении безопасности в компании?
Варианты ответа:

1. Поддержка высшего руководства
2. Эффективные защитные меры и методы их внедрения
3. Актуальные и адекватные политики и процедуры безопасности
4. Проведение тренингов по безопасности для всех сотрудников

Вопрос 8:
Когда целесообразно не предпринимать никаких действий в отношении выявленных рисков?
Варианты ответа:

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

Вопрос 9:
Что такое политики безопасности?
Варианты ответа:

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

Вопрос 10:
Какая из приведенных техник является самой важной при выборе конкретных защитных мер?
Варианты ответа:

1. а) Анализ рисков
2. б) Анализ затрат / выгоды
3. в) Результаты ALE
4. г) Выявление уязвимостей и угроз, являющихся причиной риска

Вопрос 11:
Что лучше всего описывает цель расчета ALE?
Варианты ответа:

1. а) Количественно оценить уровень безопасности среды
2. б) Оценить возможные потери для каждой контрмеры
3. в) Количественно оценить затраты / выгоды
4. г) Оценить потенциальные потери от угрозы в год

Вопрос 12:
Тактическое планирование – это:
Варианты ответа:

1. а) Среднесрочное планирование
2. б) Долгосрочное планирование
3. в) Ежедневное планирование

4. г) Планирование на 6 месяцев

Вопрос 13:
Что является определением воздействия (exposure) на безопасность?
Варианты ответа:

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

Вопрос 14:
Эффективная программа безопасности требует сбалансированного применения:
Варианты ответа:

1. Технических и нетехнических методов
2. Контрмер и защитных механизмов
3. Физической безопасности и технических средств защиты
4. Процедур безопасности и шифрования

Вопрос 15:
Функциональность безопасности определяет ожидаемую работу механизмов безопасности, а гарантии определяют:
Варианты ответа:

1. Внедрение управления механизмами безопасности
2. Классификацию данных после внедрения механизмов безопасности
3. Уровень доверия, обеспечиваемый механизмом безопасности
4. Соотношение затрат / выгод

Вопрос 16:
Какое утверждение является правильным, если взглянуть на разницу в целях безопасности для коммерческой и военной организации?
Варианты ответа:

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

Вопрос 17:
Как рассчитать остаточный риск?
Варианты ответа:

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

Вопрос 18:
Что из перечисленного не является целью проведения анализа рисков?
Варианты ответа:

1. Делегирование полномочий
2. Количественная оценка воздействия потенциальных угроз
3. Выявление рисков
4. Определение баланса между воздействием риска и стоимостью необходимых контрмер

Вопрос 19:
Что из перечисленного не является задачей руководства в процессе внедрения и сопровождения безопасности?
Варианты ответа:

1. Поддержка
2. Выполнение анализа рисков
3. Определение цели и границ
4. Делегирование полномочий

Вопрос 20:
Почему при проведении анализа информационных рисков следует привлекать к этому специалистов из различных подразделений компании?
Варианты ответа:

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

Вопрос 21:
Что является наилучшим описанием количественного анализа рисков?
Варианты ответа:

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

Вопрос 22:
Почему количественный анализ рисков в чистом виде не достижим?
Варианты ответа:

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

Вопрос 23:
Если используются автоматизированные инструменты для анализа рисков, почему все равно требуется так много времени для проведения анализа?
Варианты ответа:

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

Вопрос 24:

Какой из следующих законодательных терминов относится к компании или человеку, выполняющему необходимые действия, и используется для определения обязательств?
Варианты ответа:

1. Стандарты
2. Должный процесс (Due process)
3. Должная забота (Due care)
4. Снижение обязательств

Вопрос 25:
Что такое CobiT и как он относится к разработке систем информационной безопасности и программ безопасности?
Варианты ответа:

1. Список стандартов, процедур и политик для разработки программы безопасности
2. Текущая версия ISO 17799
3. Структура, которая была разработана для снижения внутреннего мошенничества в компаниях
4. Открытый стандарт, определяющий цели контроля

Вопрос 26:
Из каких четырех доменов состоит CobiT?
Варианты ответа:

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

Вопрос 27:
Что представляет собой стандарт ISO/IEC 27799?
Варианты ответа:

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

Вопрос 28:
CobiT был разработан на основе структуры COSO. Что является основными целями и задачами COSO?
Варианты ответа:

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

Вопрос 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?
Варианты ответа:

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

Вопрос 30:
Какой из следующих методов анализа рисков пытается определить, где вероятнее всего произойдет сбой?
Варианты ответа:

1. Анализ связующего дерева
2. AS/NZS
3. NIST
4. Анализ сбоев и дефектов

Вопрос 31:
Что было разработано, чтобы помочь странам и их правительствам построить законодательство по защите персональных данных похожим образом?
Варианты ответа:

1. Безопасная OECD
2. ISOIEC

3. OECD
4. CPTED

Вопрос 32:
Символы шифруемого текста перемещаются по определенным правилам внутри шифруемого блока этого текста, это метод:
Варианты ответа:

1. гаммирования;
2. подстановки;
3. кодирования;
4. перестановки;
5. аналитических преобразований.
6. Символы шифруемого текста заменяются другими символами, взятыми из одного или нескольких алфавитов, это метод:
7. гаммирования;

Вопрос 33:
Бывают подстановки;
Варианты ответа:

1. кодирования;
2. перестановки;
3. аналитических преобразований.

Вопрос 34:
Символы шифруемого текста последовательно складываются с символами некоторой специальной последовательности, это метод:
Варианты ответа:

1. гаммирования;
2. подстановки;
3. кодирования;
4. перестановки;
5. аналитических преобразований.

Вопрос 35:
Защита информации от утечки это деятельность по предотвращению:
Варианты ответа:

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.

Вопрос 36:
Защита информации это:
Варианты ответа:

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.

Вопрос 37:
Естественные угрозы безопасности информации вызваны:
Варианты ответа:

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.

Вопрос 38:
Искусственные угрозы безопасности информации вызваны:
Варианты ответа:

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.

Вопрос 39:
К основным непреднамеренным искусственным угрозам АСОИ относится:
Варианты ответа:

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.

Вопрос 40:
К посторонним лицам нарушителям информационной безопасности относится:
Варианты ответа:

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;

Вопрос 41:

Спам, который имеет цель опорочить ту или иную фирму, компанию, политического кандидата и т.п:
Варианты ответа:

1. черный пиар;
2. фишинг;
3. нигерийские письма;
4. источник слухов;
5. пустые письма.

Вопрос 42:
Спам распространяет поддельные сообщения от имени банков или финансовых компаний, целью которых является сбор логинов, паролей и пин-кодов пользователей:
Варианты ответа:

1. черный пиар;
2. фишинг;
3. нигерийские письма;
4. источник слухов;
5. пустые письма.

Вопрос 43:
Антивирус обеспечивает поиск вирусов в оперативной памяти, на внешних носителях путем подсчета и сравнения с эталоном контрольной суммы:
Варианты ответа:

1. детектор;
2. доктор;
3. сканер;
4. ревизор;
5. сторож.

Вопрос 44:
Антивирус не только находит зараженные вирусами файлы, но и "лечит" их, т.е. удаляет из файла тело программы вируса, возвращая файлы в исходное состояние:
Варианты ответа:

1. детектор;
2. доктор;
3. сканер;

4. ревизор;
5. сторож.

Вопрос 45:
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:
Варианты ответа:

1. детектор;
2. доктор;
3. сканер;
4. ревизор;
5. сторож.

Вопрос 46:
Антивирус представляет собой небольшую резидентную программу, предназначенную для обнаружения подозрительных действий при работе компьютера, характерных для вирусов:
Варианты ответа:

1. детектор;
2. доктор;
3. сканер;
4. ревизор;
5. сторож.

Вопрос 47:
Активный перехват информации это перехват, который:
Варианты ответа:

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.

Вопрос 48:
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.

Вопрос 49:
Перехват, который основан на фиксации электромагнитных излучений, возникающих при функционировании средств компьютерной техники и коммуникаций называется:
Варианты ответа:

1. активный перехват;
2. пассивный перехват;
3. аудиоперехват;
4. видеоперехват;
5. просмотр мусора.

Вопрос 50:
Перехват, который осуществляется путем использования оптической техники называется:
Варианты ответа:

1. активный перехват;
2. пассивный перехват;
3. аудиоперехват;
4. видеоперехват;
5. просмотр мусора.

Вопрос 51:
К внутренним нарушителям информационной безопасности относится:
Варианты ответа:
клиенты;

1. пользователи системы;
2. посетители;
3. любые лица, находящиеся внутри контролируемой территории;
4. представители организаций, взаимодействующих по вопросам обеспечения жизнедеятельности организации.

5. персонал, обслуживающий технические средства.
6. сотрудники отделов разработки и сопровождения ПО;
7. технический персонал, обслуживающий здание