МИНИСТЕРСТВО НАУКИ И ВЫСШЕГО ОБРАЗОВАНИЯ РОССИЙСКОЙ ФЕДЕРАЦИИ
ФЕДЕРАЛЬНОЕ ГОСУДАРСТВЕННОЕ БЮДЖЕТНОЕ ОБРАЗОВАТЕЛЬНОЕ
УЧРЕЖДЕНИЕ ВЫСШЕГО ОБРАЗОВАНИЯ
«СЕВЕРО-КАВКАЗСКАЯ ГОСУДАРСТВЕННАЯ АКАДЕМИЯ»

«Утверждаю»
Проректор по учебной работе _____ Г.Ю. Нагорная
«30» 03 2022

РАБОЧАЯ ПРОГРАММА ДИСЦИПЛИНЫ

Кибербезопасность, цифровые риски и угрозы

Уровень образовательной программы бакалавриат

Направление подготовки 09.03.03 Прикладная информатика

Направленность (профиль) Прикладная информатика в экономике

Форма обучения очная

Срок освоения ОП 4 года

Институт Прикладной математики и информационных технологий

Кафедра разработчик РПД Прикладная информатика

Выпускающая кафедра Прикладная информатика

Начальник
учебно-методического управления _____ Семенова Л. У.

Директор института ПМиИТ _____ Тебуев Д. Б.

Заведующий выпускающей кафедрой _____ Хапаева Л. Х.

г. Черкесск, 2022 г.

СОДЕРЖАНИЕ

1. Цели освоения дисциплины……. 4
2. Место дисциплины в структуре образовательной программы..... 4
3. Планируемые результаты обучения по дисциплине ……. 5
4. Структура и содержание дисциплины 7
4.1. Объем дисциплины и виды учебной работы..... 7
4.2. Содержание дисциплины …….. 7
4.2.1. Разделы (темы) дисциплины, виды учебной деятельности и формы контроля……. 7
4.2.2. Лекционный курс ……... 8
4.2.3. Лабораторный практикум ……..... 9
4.2.4. Практические занятия..... 9
4.3. Самостоятельная работа обучающегося…..... 9
5. Перечень учебно-методического обеспечения для самостоятельной работы обучающихся по дисциплине..... 10
6. Образовательные технологии..... 13
7. Учебно-методическое и информационное обеспечение учебной дисциплины..... 14
7.1. Перечень основной и дополнительной учебной литературы 14
7.2. Перечень ресурсов информационно-телекоммуникационной сети «Интернет»..... 14
7.3. Информационные технологии, лицензионное программное обеспечение 14
8. Материально-техническое обеспечение дисциплины ……. 15
8.1. Требования к аудиториям (помещениям, местам) для проведения занятий 15
8.2. Требования к оборудованию рабочих мест преподавателя и обучающихся 15
8.3. Требования к специализированному оборудованию..... 15
9. Особенности реализации дисциплины для инвалидов и лиц с ограниченными возможностями здоровья 15
Приложение 1. Фонд оценочных средств..... 16
Приложение 2. Аннотация рабочей программы..... 41
Рецензия на рабочую программу..... 42
Лист переутверждения рабочей программы учебной дисциплины 43

1. ЦЕЛИ ОСВОЕНИЯ ДИСЦИПЛИНЫ

Целями освоения дисциплины «Кибербезопасность, цифровые риски и угрозы» являются: подготовка будущих специалистов-практиков к использованию современных методов и средств защиты информации в организационно-управленческой и аналитической деятельности.

При этом ***задачами*** дисциплины являются:

- формирование знаний о концепциях защиты информации и системах безопасности персональных компьютеров и компьютерных сетей;
- -изучить теорию и практику новейших достижений и перспектив в развития в области создания систем безопасности локальных вычислительных сетей и сети Internet;
- формирование знаний о криптографических методах зашиты информации; основах криптографии; основных методах и приемах защиты от несанкционированного доступа; о компьютерных вирусах и антивирусных программах; организационно-правовом обеспечение ИБ;
- развитие способности работать с различными информационными ресурсами и технологиями, применять основные методы, способы и средства получения, хранения, поиска, систематизации, обработки и передачи информации;
- овладение способностью соблюдать в профессиональной деятельности требования, установленные нормативными правовыми актами в области защиты государственной тайны и информационной безопасности, обеспечивать соблюдение режима секретности;
- формирование навыков выбора инструментальных средств для обработки финансовой, бухгалтерской и иной экономической информации и умения обосновывать свой выбор.

2. МЕСТО ДИСЦИПЛИНЫ В СТРУКТУРЕ ОБРАЗОВАТЕЛЬНОЙ ПРОГРАММЫ

2.1. Учебная дисциплина «Кибербезопасность, цифровые риски и угрозы» относится к части, формируемой участниками образовательных отношений Блока 1. Дисциплины (модули), имеет тесную связь с другими дисциплинами.

2.2. В таблице приведены предшествующие и последующие дисциплины, направленные на формирование компетенций дисциплины в соответствии с матрицей компетенций ОП.

Предшествующие и последующие дисциплины, направленные на формирование компетенций

№ п/п	Предшествующие дисциплины	Последующие дисциплины
1	Информационная безопасность	Производственная практика (преддипломная практика)

3. ПЛАНИРУЕМЫЕ РЕЗУЛЬТАТЫ ОБУЧЕНИЯ

Планируемые результаты освоения образовательной программы (ОП) – компетенции обучающихся определяются требованиями стандарта по направлению подготовки 09.03.03 Прикладная информатика и формируются в соответствии с матрицей компетенций ОП

№ п/п	Номер/ индекс компетенции	Наименование компетенции (или ее части)	В результате изучения дисциплины обучающиеся должны:
1	2	3	4
1.	ПК-5	Способен проводить обследование организаций, выявлять информационные потребности пользователей, формировать требования к цифровой информационной системе	ПК-5.1. Использует терминологию и формулирует задачи как в области финансовых технологий и цифровой экономики, так и в области информатики и IT-технологий ПК-5.2. Обладает навыками организации учета и управления процессом подготовки традиционных и электронных конфиденциальных документов ПК-5.7. Применяет методы выявления требований, методы и средства управления ИТ-проектами

4. СТРУКТУРА И СОДЕРЖАНИЕ ДИСЦИПЛИНЫ

4.1. ОБЪЕМ ДИСЦИПЛИНЫ И ВИДЫ УЧЕБНОЙ РАБОТЫ

Вид учебной работы		**Всего часов**	**Семестр**
			№ 8
			Часов
1		2	3
Аудиторная контактная работа (всего)		40	40
В том числе:			
Лекции (Л)		16	16
Практические занятия (ПЗ), Семинары (С)			
Лабораторные работы (ЛР)		24	24
Контактная внеаудиторная работа, в том числе:		**2**	**2**
индивидуальные и групповые консультации		2	2
Самостоятельная работа обучающегося (СРО) (всего)		39	39
Работа с лекциями		8	8
Подготовка к лабораторным занятиям		6	6
Работа с книжными источниками		8	8
Работа с электронными источниками		8	8
Подготовка к контрольной работе		5	5
Подготовка к текущему контролю (ПТК)		2	2
Подготовка к промежуточному контролю (ППК)		2	2
Промежуточная аттестация	Экзамен (Э)	Э (27)	Э (27)
	Прием экз., час.	0,5	0,5
	Консультация, час.	2	2
	СРО, час.	24,5	24,5
ИТОГО: Общая трудоемкость	**Часов**	108	108
	зач. ед.	3	3

4.2. СОДЕРЖАНИЕ ДИСЦИПЛИНЫ

4.2.1. Разделы (темы) дисциплины, виды учебной деятельности и формы контроля

№ п/п	№ семестра	Наименование раздела(темы) дисциплины	Виды учебной деятельности, включая самостоятельную работу обучающегося (в часах)					Формы текущей и промежуточной аттестации
			Л	ЛР	ПЗ	СРО	всего	
1	2	3	4	5	6	7	8	9
1.	8	Раздел 1. Введение. Основные понятия и определения	6	6		12	24	Отчет по лабораторной работе, устный опрос, тестирование, контрольная работа
2	8	Раздел 2. Безопасность информационных систем	6	14		15	35	Отчет по лабораторной работе, устный опрос, тестирование, контрольная работа
	8	Раздел 3. Киберпреступность и способы ее предотвращения	4	4		12	20	Отчет по лабораторной работе, устный опрос, тестирование, контрольная работа
3.	8	Контактная внеаудиторнаяработа					27	Индивидуальные и групповые консультации
4.	8	Промежуточная аттестация					2	Экзамен
Итого часов в 8 семестре:			16	24		39	108	
Всего:			16	24		39	108	

4.2.2. Лекционный курс

№ п/п	Наименование раздела дисциплины	Наименование темы лекции	Содержание лекции	Всего часов
1	2	3	4	5
Семестр 8				
1.	Раздел 1. Основные понятия в области кибербезопасности.	Тема 1.1. Основные понятия в области кибербезопасности.	1. Основные термины и понятия. Угрозы кибербезопасности. 2. Угрозы кибербезопасности. 3. Уровни и стандарты информационной безопасности. 4. Разработка требований к системе и структуры системы кибербезопасности 5. Анализ рисков безопасности разработанной системы 6. Разработка документации для системы безопасности	**6**
2.	Раздел 2. Безопасность информационных систем	Тема 2.1. Безопасность информационных систем	1.Вредоносное программное обеспечение и защита от него. 2. Обеспечение доступности и защищенности информационных систем. 3. Разработка программы криптозащиты канала связи 4. Разработка программы криптозащиты данных, хранящихся на носителе	**6**
3.	Раздел 3. Киберпреступность и способы ее предотвращения.	Тема 3.1. Киберпреступность и способы ее предотвращения.	1.Проект модели угроз кибербезопасности. 2.Разработка должностных инструкций по внедрению иэксплуатации ПО, обеспечивающего кибербезопасность	**4**
	ИТОГО часов в семестре:			**16**

4.2.3. Лабораторный практикум

№ п / п	Наименование раздела дисциплины	Наименование лабораторных работ	Всего часов
1.	2	3	4
1.	Раздел 1. Основные понятия в области кибербезопасности.	Сравнение данных с помощью хэш-функции	**6**
		Создание и сохранение надежных паролей	
		Резервное копирование данных во внешнее хранилище	
2.	Раздел 2. Безопасность информационных систем	Организация защиты рабочих станций и информационных систем, в соответствии с требованиями национальных стандартов	**14**
		Настройка функционала защиты информации при эксплуатации программно-аппаратных комплексов.	
		Способы защиты от утечки информации по техническим каналам.	
		Защита графического файла с помощью цифрового водяного знака с применением LSB алгоритма.	
		Метод Куттера-Джордана-Боссена	
		Симметричные криптосистемы шифрования.	
		Асимметричные криптосистемы шифрования.	
3.	Раздел 3. Киберпреступность и способы ее предотвращения	Электронная цифровая подпись.	**4**
	ИТОГО:		**24**

4.2.4. Практические занятия не предусмотрены

4.3. САМОСТОЯТЕЛЬНАЯ РАБОТА ОБУЧАЮЩЕГОСЯ

№ п/п	Наименование раздела (темы) дисциплины	№ п/п	Виды СРО	Всего часов
1	2	3	4	5
Семестр 8				
1.	Раздел 1. Основные понятия в области кибербезопасности.	1.1.	Проработка лекций - включает чтение конспекта лекций, профессиональной литературы, периодических изданий. Подготовка к лабораторному занятию. Подготовка к тестированию Подготовка к контрольной работе Внеаудиторная контактная работа	12
2.	Раздел 2. Безопасность информационных систем	2.1.	Проработка лекций - включает чтение конспекта лекций, профессиональной литературы, периодических изданий. Подготовка к лабораторному занятию. Подготовка к тестированию Подготовка к контрольной работе	15
3.	Раздел 3. Киберпреступность и способы ее предотвращения	3.1	Проработка лекций - включает чтение конспекта лекций, профессиональной литературы, периодических изданий. Подготовка к лабораторному занятию. Подготовка к тестированию Подготовка к контрольной работе Подготовка к текущему контролю (ПТК) Подготовка к промежуточному контролю (ППК)	12
ИТОГО часов в семестре:				39

5. ПЕРЕЧЕНЬ УЧЕБНО-МЕТОДИЧЕСКОГО ОБЕСПЕЧЕНИЯ ДЛЯСАМОСТОЯТЕЛЬНОЙ РАБОТЫ ОБУЧАЮЩИХСЯ ПО ДИСЦИПЛИНЕ

5.1. Методические указания для подготовки обучающегося к лекционным занятиям

На лекциях рекомендуется деятельность обучающегося в форме активного слушания, т.е. предполагается возможность задавать вопросы на уточнение понимания темы и рекомендуется конспектирование основных положений лекции. Основная дидактическая цель лекции — обеспечение ориентировочной основы для дальнейшего усвоения учебного материала.

В ходе лекционных занятий необходимо вести конспектирование учебного материала. Обращать внимание на категории, формулировки, раскрывающие содержание тех или иных явлений и процессов, научные выводы и практические рекомендации. После лекции необходимо доработать свой конспект лекции, делая в нем соответствующие записи из литературы, рекомендованной преподавателем и предусмотренной рабочей программой.

Специфической чертой изучения данного курса является то, что приобретение умений и навыков работы невозможно без систематической тренировки, которая осуществляется на практических занятиях. Консультации проводятся с целью оказания помощи обучающимся в изучении учебного материала, подготовки их к практическим

занятиям.

5.2. Методические указания для подготовки обучающихся к лабораторным занятиям

Лабораторные работы сопровождают и поддерживают лекционный курс. Лекция закладывает основы знаний по предмету в обобщенной форме, а лабораторные занятия направлены на расширение и детализацию этих знаний, на выработку и закрепление навыков профессиональной деятельности. Подготовка к лабораторным занятиям предполагает предварительную самостоятельную работу обучающихся в соответствии с методическими разработками по каждой запланированной теме.

Лабораторные занятия позволяют интегрировать теоретические знания и формировать практические умения и навыки обучающихся в процессе учебной деятельности. Структура и последовательность занятий: на первом, вводном, занятии проводится инструктаж обучающихся по охране труда, технике безопасности и правилам работы в лаборатории по инструкциям утвержденного образца с фиксацией результатов в журнале инструктажа. Обучающиеся также знакомятся с основными требованиями преподавателя по выполнению учебного плана, с графиком прохождения лабораторных занятий, с графиком прохождения контрольных заданий, с основными формам отчетности по выполненным работам и заданиям.

Лабораторные работы выполняются в соответствии с методическими указаниями. Структура лабораторного занятия:

- Объявление темы, цели и задач занятия.
- Проверка теоретической подготовки обучающихся к лабораторному занятию.
- Выполнение лабораторной работы.
- Подведение итогов занятия (формулирование выводов).
- Оформление отчета.
- Защита работы преподавателю дисциплины.

5.3. Методические указания для подготовки обучающихся к практическим занятиям *(не предусмотрены учебным планом)*

5.2. Методические указания по самостоятельной работе обучающихся Работа с литературными источниками и интернет ресурсами

В процессе подготовки к практическим занятиям, обучающимся необходимо обратить особое внимание на самостоятельное изучение рекомендованной учебно-методической (а также научной и популярной) литературы.

Самостоятельная работа с учебниками, учебными пособиями, научной, справочной и популярной литературой, материалами периодических изданий и Интернета, статистическими данными является наиболее эффективным методом получения знаний, позволяет значительно активизировать процесс овладения информацией, способствует более глубокому усвоению изучаемого материала, формирует у обучающихся свое отношение к конкретной проблеме.

Более глубокому раскрытию вопросов способствует знакомство с дополнительной литературой, рекомендованной преподавателем по каждой теме семинарского или практического занятия, что позволяет обучающимся проявить свою индивидуальность в рамках выступления на данных занятиях, выявить широкий спектр мнений по изучаемой проблеме.

В качестве мероприятий по текущему контролю в соответствии с РПД дисциплины возможно проведение аудиторных контрольных работ и прохождение промежуточного тестирования.

Для успешного прохождения этого этапа обучения необходимо:

1. Внимательно прочитать конспекты, составленные на учебном занятии.

2. Изучить тематику контрольной работы по рекомендованным литературнымисточникам (учебники, учебные пособия).

3. Ответить на контрольные вопросы, выданные преподавателем для подготовки кконтрольной работе.

4. Потренироваться в решении задач, изученных на практических занятиях.

5. Составить опорный конспект по контролируемым темам.При подготовке к тестированию необходимо:

− проработать информационный материал по дисциплине,

− четко выяснить все условия тестирования заранее: сколько тестов будет предложено, сколько времени отводится на тестирование, какова система оценки результатов и т.д.

При прохождении тестирования необходимо:

− внимательно и до конца прочитать вопрос и предлагаемые варианты ответов, выбрать правильные (их может быть несколько);

− в процессе решения желательно применять несколько подходов в решении задания (это позволяет максимально гибко оперировать методами решения, находя каждый раз оптимальный вариант);

− не тратить много времени на «трудный вопрос», переходить к другим тестам, вернувшись к нему в конце;

− оставить время для проверки ответов, чтобы избежать механических ошибок.

Методические указания по подготовке к устному опросу

Целью устного собеседования являются обобщение и закрепление изученного курса. Обучающимся предлагаются для освещения сквозные концептуальные проблемы. При подготовке следует использовать лекционный материал и учебную литературу. Для более глубокого постижения курса и более основательной подготовки рекомендуется познакомиться с указанной дополнительной литературой. Готовясь к семинару, обучающийся должен, прежде всего, ознакомиться с общим планом семинарского занятия. Следует внимательно прочесть свой конспект лекции по изучаемой теме и рекомендуемую к теме семинара литературу. При этом важно научиться выделять в рассматриваемой проблеме самое главное и сосредотачивать на нем основное внимание при подготовке. С незнакомыми терминами и понятиями следует ознакомиться в предлагаемом глоссарии, словаре или энциклопедии.

Ответ на каждый вопрос из плана семинарского занятия должен быть доказательным и аргументированным, обучающемуся нужно уметь отстаивать свою точку зрения. Для этого следует использовать документы, монографическую, учебную и справочную литературу. Активно участвуя в обсуждении проблем на семинарах обучающиеся учатся последовательно мыслить, логически рассуждать, внимательно слушать своих товарищей, принимать участие в спорах и дискуссиях. Для успешной подготовки к устному опросу, обучающийся должен законспектировать рекомендуемую литературу, внимательно осмыслить фактический материал и сделать выводы. Обучающемуся надлежит хорошо подготовиться, чтобы иметь возможность грамотно и полно ответить на заданные ему вопросы, суметь сделать выводы и показать значимость данной проблемы для изучаемого курса. Обучающемуся необходимо также дать анализ той литературы, которой он воспользовался при подготовке к устному опросу на семинарском занятии.

При подготовке, обучающийся должен правильно оценить вопрос, который он взял для выступления к семинарскому занятию. Но для того чтобы правильно и четко ответить на поставленный вопрос, необходимо правильно уметь пользоваться учебной и дополнительной литературой.

Перечень требований к любому выступлению обучающегося примерно таков:

связь выступления с предшествующей темой или вопросом.

раскрытие сущности проблемы.

методологическое значение для научной, профессиональной и практической деятельности.

Разумеется, обучающийся не обязан строго придерживаться такого порядка изложения, но все аспекты вопроса должны быть освещены, что обеспечит выступлению необходимую полноту и завершенность.

Приводимые участником семинара примеры и факты должны быть существенными, по возможности перекликаться с профилем обучения.

Выступление обучающегося должно соответствовать требованиям логики. Четкое вычленение излагаемой проблемы, ее точная формулировка, неукоснительная последовательность аргументации именно данной проблемы, без неоправданных отступлений от нее в процессе обоснования, безусловная доказательность, непротиворечивость и полнота аргументации, правильное и содержательное использование понятий и терминов.

Методические рекомендации прохождения тестирования

Подготовку к итоговому тестированию необходимо осуществлять поэтапно.

На первом этапе необходимо повторить основные положения всех тем, детально разбирая наиболее сложные моменты. Непонятные вопросы необходимо выписывать, чтобы по ним можно было проконсультироваться с преподавателем перед прохождением итогового тестирования. Подготовку по темам каждой дидактической единицы целесообразно производить отдельно. На этом этапе необходимо использовать материалы лекционного курса, материалы семинарских занятий, тестовые задания для текущего контроля знаний, а также презентации лекционного курса.

На втором этапе подготовки предлагается без повторения теоретического материала дать ответы тестовые задания для рубежного контроля знаний. Если ответы на какие-то вопросы вызвали затруднение, необходимо еще раз повторить соответствующий теоретический материал.

Наконец, третий этап подготовки необходимо осуществить непосредственно накануне теста. На данном этапе необходимо аккуратно просмотреть весь лекционный курс.

В случае, если результаты выполнения тестового задания оказались неудовлетворительными, необходимо зафиксировать темы, на вопросы по которым были даны неверные ответы, и еще раз углубленно повторить соответствующие темы в соответствии с указанными выше тремя этапами подготовки к тестированию.

Методические указания к выполнению контрольной работы

Контрольной работе как одной из форм самостоятельной учебно-исследовательской работы отводится особая роль при формировании компетенции будущего специалиста и бакалавра. Здесь обучающийся демонстрирует применение полученных знаний для создания приложений, решающих конкретные поставленные перед ним задачи. Обучающийся предъявляет преподавателю несколько версий программ, как правило, в электронном виде и получает от преподавателя положительное заключение о результате, либо замечания и предложения по корректировке программы. Программа должна предъявляться в виде, допускающем быстрый переход к ее компиляции, т.е. не допускается передача в виде изображения. Принимаются любые варианты программы, решающие исходную задачу. Преподаватель при приеме приводящей к верному результату программы зачитывает ее как исполненную, но может дать рекомендации по ее улучшению.

Промежуточная аттестация

По итогам 8 семестра проводится экзамен. При подготовке к сдаче Экзамена

рекомендуется пользоваться материалами практических занятий и материалами, изученными в ходе текущей самостоятельной работы.

Экзамен проводится в устной или письменной форме, включает подготовку и ответы обучающегося на теоретические вопросы. По итогам экзамена выставляется оценка.

По итогам обучения проводится экзамен, к которому допускаются обучающиеся, имеющие положительные результаты по защите практических работ.

Методические рекомендации по подготовке к экзамену

Экзамен – это форма итоговой отчетности студента по изученной дисциплине. По решению кафедры экзамен может проводиться в нескольких формах – устной по билетам. Главная задача проведения экзамена – проверка знаний, навыков и умений студента, по прослушанной дисциплине.

Огромную роль в успешной подготовке к экзамену играет правильная организация подготовки к нему. Рекомендуется при подготовке к экзамену опираться на следующий план:

просмотреть программу курса, с целью выявления наиболее проблемных тем, вопросов, которые могут вызвать трудности при подготовке к экзамену.

прорешать задачу, предложенные в учебно-методическом комплексе. При этом для эффективного закрепления информации первый раз без использования учебных материалов и нормативно-правовых актов, второй раз с их использованием.

При выполнении первых двух пунктов плана студент получит возможность оценить свои знания и навыки по прослушанной дисциплине и сориентироваться при планировании объема подготовки.

темы необходимо изучать последовательно, внимательно обращая внимание на описание вопросов, которые раскрывают ее содержание. Начинать необходимо с первой темы.

после работы над первой темой необходимо ответить на контрольные вопросы к теме и решить тестовые задания к ней.

после изучения всех тем студенту рекомендуется ответить на контрольные вопросы по всему курсу.

6. ОБРАЗОВАТЕЛЬНЫЕ ТЕХНОЛОГИИ

№ п/п	№ семестра	Виды учебной работы	Образовательные технологии	Всего часов
1	2	3	4	
1	8	*Лекция 3.* Киберпреступность и способы ее предотвращения	Презентация. Учебно-исследовательская работа	2
2		*Лабораторная работа 3.* Резервное копирование данных во внешнее хранилище	Учебно-исследовательская работа. Компьютерная симуляция	2
3		*Лабораторная работа 7.* Защита графического файла с помощью цифрового водяного знака с применением LSB алгоритма.	Учебно-исследовательская работа. Компьютерная симуляция	2

4		*Лабораторная работа 11.* Электронная цифровая подпись.	Учебно-исследовательская работа. Компьютерная симуляция.	2

7. УЧЕБНО-МЕТОДИЧЕСКОЕ И ИНФОРМАЦИОННОЕ ОБЕСПЕЧЕНИЕДИСЦИПЛИНЫ

7.1. Перечень основной и дополнительной учебной литературы

	Список основной литературы
1.	Басыня, Е. А. Сетевая информационная безопасность : учебник / Е. А. Басыня. — Москва : Национальный исследовательский ядерный университет «МИФИ», 2023. — 224 с. — ISBN 978-5-7262-2949-2. — Текст : электронный // Цифровой образовательный ресурс IPR SMART : [сайт]. — URL: https://www.iprbookshop.ru/132693.html (дата обращения: 06.09.2023). — Режим доступа: для авторизир. пользователей
2.	Киренберг, А. Г. Системное администрирование и информационная безопасность сетей ЭВМ : учебное пособие / А. Г. Киренберг. — Кемерово : Кузбасский государственный технический университет имени Т.Ф. Горбачева, 2022. — 119 с. — ISBN 978-5-00137-292-9. — Текст : электронный // Цифровой образовательный ресурс IPR SMART : [сайт]. — URL: https://www.iprbookshop.ru/128406.html (дата обращения: 21.02.2023). — Режим доступа: для авторизир. пользователей
3.	Семенов, Ю. А. Процедуры, диагностики и безопасность в Интернет : учебное пособие / Ю. А. Семенов. — 4-е изд. — Москва : Интернет-Университет Информационных Технологий (ИНТУИТ), Ай Пи Ар Медиа, 2022. — 581 с. — ISBN 978-5-4497-1653-8. — Текст : электронный // Цифровой образовательный ресурс IPR SMART : [сайт]. — URL: https://www.iprbookshop.ru/120489.html (дата обращения: 03.07.2023). — Режим доступа: для авторизир. пользователей
4.	Киренберг, А. Г. Информационная безопасность современных операционных систем : учебное пособие / А. Г. Киренберг. — Кемерово : Кузбасский государственный технический университет имени Т.Ф. Горбачева, 2022. — 138 с. — ISBN 978-5-00137-320-9. — Текст : электронный // Цифровой образовательный ресурс IPR SMART : [сайт]. — URL: https://www.iprbookshop.ru/128393.html (дата обращения: 21.02.2023). — Режим доступа: для авторизир. пользователей
5.	Мэйволд, Э. Безопасность сетей : учебное пособие / Э. Мэйволд. — 3-е изд. — Москва : Интернет-Университет Информационных Технологий (ИНТУИТ), Ай Пи Ар Медиа, 2021. — 571 с. — ISBN 978-5-4497-0863-2. — Текст : электронный // Цифровой образовательный ресурс IPR SMART : [сайт]. — URL: https://www.iprbookshop.ru/101992.html (дата обращения: 22.09.2022). — Режим доступа: для авторизир. пользователей
6.	Ревнивых, А. В. Информационная безопасность в организациях : учебное пособие / А. В. Ревнивых. — Москва : Ай Пи Ар Медиа, 2021. — 83 с. — ISBN 978-5-4497-1164-9. — Текст : электронный // Цифровой образовательный ресурс IPR SMART : [сайт]. — URL: https://www.iprbookshop.ru/108227.html (дата обращения: 30.10.2023). — Режим доступа: для авторизир. пользователей. - DOI: https://doi.org/10.23682/108227
7.	Куликов, С. С. Информационная безопасность глобальных компьютерных сетей : практикум / С. С. Куликов. — Воронеж : Воронежский государственный технический университет, ЭБС АСВ, 2021. — 66 с. — ISBN 978-5-7731-0970-9. — Текст : электронный // Цифровой образовательный ресурс IPR SMART : [сайт]. — URL: https://www.iprbookshop.ru/118613.html (дата обращения: 30.10.2023). — Режим доступа: для авторизир. пользователей
8.	Куликов, С. С. Информационная безопасность локальных компьютерных сетей : практикум / С. С. Куликов. — Воронеж : Воронежский государственный технический университет, ЭБС АСВ, 2021. — 57 с. — ISBN 978-5-7731-0969-3. — Текст : электронный // Цифровой образовательный ресурс IPR SMART : [сайт]. — URL:

	https://www.iprbookshop.ru/118614.html (дата обращения: 30.10.2023). — Режим доступа: для авторизир. пользователей
9.	Фороузан, Б. А. Криптография и безопасность сетей : учебное пособие / Б. А. Фороузан ; под редакцией А. Н. Берлина. — 3-е изд. — Москва : Интернет-Университет Информационных Технологий (ИНТУИТ), Ай Пи Ар Медиа, 2021. — 776 с. — ISBN 978-5-4497-0946-2. — Текст : электронный // Цифровой образовательный ресурс IPR SMART : [сайт]. — URL: https://www.iprbookshop.ru/102017.html (дата обращения: 22.09.2022). — Режим доступа: для авторизир. пользователей
10.	Брюхомицкий, Ю. А. Безопасность информационных технологий. В 2 частях. Ч.1 : учебное пособие / Ю. А. Брюхомицкий. — Ростов-на-Дону, Таганрог : Издательство Южного федерального университета, 2020. — 171 с. — ISBN 978-5-9275-3571-2 (ч.1), 978-5-9275-3526-2. — Текст : электронный // Цифровой образовательный ресурс IPR SMART : [сайт]. — URL: https://www.iprbookshop.ru/107943.html (дата обращения: 28.09.2023). — Режим доступа: для авторизир. пользователей
11.	Суворова, Г. М. Информационная безопасность : учебное пособие / Г. М. Суворова. — Саратов : Вузовское образование, 2019. — 214 с. — ISBN 978-5-4487-0585-4. — Текст : электронный // Цифровой образовательный ресурс IPR SMART : [сайт]. — URL: https://www.iprbookshop.ru/86938.html (дата обращения: 30.10.2023). — Режим доступа: для авторизир. пользователей. - DOI: https://doi.org/10.23682/86938
12.	Шаньгин, В. Ф. Информационная безопасность и защита информации / В. Ф. Шаньгин. — 2-е изд. — Саратов : Профобразование, 2019. — 702 с. — ISBN 978-5-4488-0070-2. — Текст : электронный // Цифровой образовательный ресурс IPR SMART : [сайт]. — URL: https://www.iprbookshop.ru/87995.html (дата обращения: 30.10.2023). — Режим доступа: для авторизир. пользователей
13.	Шаньгин, В. Ф. Информационная безопасность и защита информации / В. Ф. Шаньгин. — 2-е изд. — Саратов : Профобразование, 2019. — 702 с. — ISBN 978-5-4488-0070-2. — Текст : электронный // Цифровой образовательный ресурс IPR SMART : [сайт]. — URL: https://www.iprbookshop.ru/87995.html (дата обращения: 30.10.2023). — Режим доступа: для авторизир. пользователей
14.	Петров, А. А. Компьютерная безопасность. Криптографические методы защиты / А. А. Петров. — 2-е изд. — Саратов : Профобразование, 2019. — 446 с. — ISBN 978-5-4488-0091-7. — Текст : электронный // Цифровой образовательный ресурс IPR SMART : [сайт]. — URL: https://www.iprbookshop.ru/87998.html (дата обращения: 30.10.2023). — Режим доступа: для авторизир. пользователей
	Список дополнительной литературы
1.	Бойко, Г. М. Информационные технологии. Практикум для обучающихся по направлению подготовки 20.03.01 Техносферная безопасность : практикум / Г. М. Бойко. — Железногорск : Сибирская пожарно-спасательная академия ГПС МЧС России, 2020. — 109 с. — Текст : электронный // Цифровой образовательный ресурс IPR SMART : [сайт]. — URL: https://www.iprbookshop.ru/103329.html (дата обращения: 30.10.2023). — Режим доступа: для авторизир. пользователей
2.	Гаенко, В. П. Безопасность технических систем. Методологические аспекты теории, методы анализа и управления безопасностью : монография / В. П. Гаенко, В. Е. Костюков, В. Н. Фомченко. — Саров : Российский федеральный ядерный центр – ВНИИЭФ, 2020. — 329 с. — ISBN 978-5-9515-0452-4. — Текст : электронный // Цифровой образовательный ресурс IPR SMART : [сайт]. — URL: https://www.iprbookshop.ru/101918.html (дата обращения: 04.10.2023). — Режим доступа: для авторизир. пользователей
3.	Моргунов, А. В. Информационная безопасность : учебно-методическое пособие / А. В. Моргунов. — Новосибирск : Новосибирский государственный технический университет, 2019. — 83 с. — ISBN 978-5-7782-3918-0. — Текст : электронный // Цифровой образовательный ресурс IPR SMART : [сайт]. — URL: https://www.iprbookshop.ru/98708.html

	(дата обращения: 30.10.2023). — Режим доступа: для авторизир. пользователей

7.2. Перечень ресурсов информационно-телекоммуникационной сети «Интернет»
http://elibrary.ru - Научная электронная библиотека.

7.3 Информационные технологии

В компьютерном классе должны быть установлены средства:

Лицензионное программное обеспечение	Реквизиты лицензий/ договоров
Microsoft Azure Dev Tools for Teaching 1. Windows 7, 8, 8.1, 10 2. Visual Studio 2008, 2010, 2013, 2019 5. Visio 2007, 2010, 2013 6. Project 2008, 2010, 2013 7. Access 2007, 2010, 2013 и т. д.	Идентификатор подписчика: 1203743421 Срок действия: 30.06.2022 (продление подписки)
MS Office 2003, 2007, 2010, 2013	Сведения об Open Office: 63143487, 63321452, 64026734, 6416302, 64344172, 64394739, 64468661, 64489816, 64537893, 64563149, 64990070, 65615073 Лицензия бессрочная
Антивирус Dr.Web Desktop Security Suite	Лицензионный сертификат Серийный № 8DVG-V96F-H8S7-NRBC Срок действия: с 20.10.2022 до 22.10.2023
Консультант Плюс	Договор № 272-186/С-23-01 от 20.12.2022 г.
Цифровой образовательный ресурс IPR SMART	Лицензионный договор № 10423/23П от 30.06.2023 г. Срок действия: с 01.07.2023 г. до 01.07.2024г.
Бесплатное ПО:	OpenServer, Notepad ++, MySQL, WinDjView, Sumatra PDF, 7-Zip

8. Материально-техническое обеспечение дисциплины

8.1. Требования к аудиториям (помещениям, местам) для проведения занятий

1. Учебная аудитория для проведения занятий лекционного типа.
Специализированная мебель:
Кафедра напольная - 1шт., стул преподавательский мягкий - 1шт., парты - 18шт., стульямягкие -32шт., стулья ученические-11 шт., доска меловая - 1шт.
Набор демонстрационного оборудования и учебно-наглядных пособий, обеспечивающихтематические иллюстрации:
Интерактивная система – 1
шт.Системный блок -1 шт.
Проектор – 1шт.

2. Лаборатория сетевых технологий. Лаборатория архитектуры ЭВМ.
Специализированная мебель:
Парты - 5шт., стулья - 26шт., доска - 1шт., лаб. столы - 6шт., стол преподавательский -2шт.
Лабораторное оборудование, технические средства обучения, служащие для предоставления учебной информации большой аудитории:

ПК – 8 шт.

3. Помещение для самостоятельной работы

Библиотечно-издательский центр

Отдел обслуживания печатными изданиями: комплект: проекционный, мультимедийное оборудование: экран настенный , проектор, ноутбук, рабочие столы, стулья .

Отдел обслуживания электронными изданиями: интерактивная система , монитор, сетевой терминал, персональный компьютер ,МФУ, принтер , рабочие столы, стулья.

Информационно-библиографический отдел: персональный компьютер, сканер, МФУ, рабочие столы, стулья

8.2. Требования к оборудованию рабочих мест преподавателя и обучающихся

1. рабочее место преподавателя, оснащенное компьютером.
2. рабочие места обучающихся, оснащенные компьютером.

8.3. Требования к специализированному оборудованию

Нет

9. ОСОБЕННОСТИ РЕАЛИЗАЦИИ ДИСЦИПЛИНЫ ДЛЯ ИНВАЛИДОВ И ЛИЦ СОГРАНИЧЕННЫМИ ВОЗМОЖНОСТЯМИ ЗДОРОВЬЯ

Для обеспечения образования инвалидов и обучающихся с ограниченными возможностями здоровья разрабатывается (в случае необходимости) адаптированная образовательная программа, индивидуальный учебный план с учетом особенностей их психофизического развития и состояния здоровья, в частности применяется индивидуальный подход к освоению дисциплины, индивидуальные задания: рефераты, письменные работы и, наоборот, только устные ответы и диалоги, индивидуальные консультации, использование диктофона и других записывающих средств для воспроизведения лекционного и семинарского материала.

В целях обеспечения обучающихся инвалидов и лиц с ограниченными возможностями здоровья комплектуется фонд основной учебной литературой, адаптированной к ограничению электронных образовательных ресурсов, доступ к которым организован в БИЦ Академии. В библиотеке проводятся индивидуальные консультации для данной категории пользователей, оказывается помощь в регистрации и использовании сетевых и локальных электронных образовательных ресурсов, предоставляются места в читальном зале.

Приложение 1

ФОНД ОЦЕНОЧНЫХ СРЕДСТВ

ПО УЧЕБНОЙ ДИСЦИПЛИНЕ Кибербезопасность, цифровые риски и угрозы

ПАСПОРТ ФОНДА ОЦЕНОЧНЫХ СРЕДСТВ ПО УЧЕБНОЙ ДИСЦИПЛИНЕ

1. Компетенции, формируемые в процессе изучения дисциплины

Индекс	Формулировка компетенции
ПК-5	Способен проводить обследование организаций, выявлять информационные потребности пользователей, формировать требования к цифровой информационной системе

2. Этапы формирования компетенции в процессе освоения дисциплины

Основными этапами формирования указанных компетенций при изучении обучающимися дисциплины являются последовательное изучение содержательно связанных между собой разделов (тем) учебных занятий. Изучение каждого раздела (темы) предполагает овладение обучающимися необходимыми компетенциями. Результат аттестации обучающихся на различных этапах формирования компетенций показывает уровень освоения компетенций обучающимися.

Этапность формирования компетенций прямо связана с местом дисциплины в образовательной программе.

Разделы (темы) дисциплины	**Формируемые компетенции (коды)**
	ПК-5
Раздел 1. Основные понятия в области кибербезопасности.	+
Раздел 2. Безопасность информационных систем	+
Раздел 3. Киберпреступность и способы ее предотвращения	+

3. Показатели, критерии и средства оценивания компетенций, формируемых в процессе изучения дисциплины

ПК – 5 Способен проводить обследование организаций, выявлять информационные потребности пользователей, формировать требования к цифровой информационной системе

Индикаторы достижения компетенций	Критерии оценивания результатов обучения				Средства оценивания результатов обучения	
	неудовлетв	удовлетв	хорошо	отлично	Текущий контроль	Промежуточная аттестация
ПК-5.1 Использует терминологию и формулирует задачи как в области финансовых технологий и цифровой экономики, так и в области информатики и IT-технологий	Не знает терминологию и формулирует задачи как в области финансовых технологий и цифровой экономики, так и в области информатики и IT-технологий. Допускает существенные ошибки при раскрытии содержания построения защищенного документооборота	Демонстрирует частичные знания терминологии и формулирует задачи как в области финансовых технологий и цифровой экономики, так и в области информатики и IT-технологий	Сформированные, но содержащие отдельные пробелы в терминологии и формулирует задачи как в области финансовых технологий и цифровой экономики, так и в области информатики и IT-технологий	Сформированные систематические представления в терминологии и формулирует задачи как в области финансовых технологий и цифровой экономики, так и в области информатики и IT-технологий	Защита лабораторных работ, контрольные вопросы, контрольная работа, тестирование	Экзамен
ПК- 5.2 Обладает навыками организации учета и управления процессом подготовки традиционных и электронных конфиденциальных документов	Не умеет организовать учет и управление процессом подготовки традиционных и электронных конфиденциальных документов . Фрагментарное использование навыков защиты конфиденциальной информации.	В целом успешное, но не систематическое использование навыков организации учета и управления процессом подготовки традиционных и электронных конфиденциальных документов	В целом успешное, но содержащее отдельные пробелы использование навыков организации учета и управления процессом подготовки традиционных и электронных конфиденциальных документов.	Сформированное умение использовать навыки организации учета и управления процессом подготовки традиционных и электронных конфиденциальных документов	Защита лабораторных работ, контрольные вопросы, контрольная работа, тестирование	Экзамен
ПК-5.7. Применяет методы выявления требований, методы и средства управления ИТ-проектами.	Не применяет методы выявления требований, методы и средства управления ИТ-проектами.	В целом успешное, но не систематическое использование методов выявления требований, методов и средств управления ИТ-проектами.	В целом успешное, но содержащее отдельные пробелы использование методов выявления требований, методов и средств управления ИТ-проектами.	Сформированное умение использовать методы выявления требований, методов и средств управления ИТ-проектами, навыки защиты конфиденциальной информации.	Защита лабораторных работ, контрольные вопросы, контрольная работа, тестирование	Экзамен

4. Комплект контрольно-оценочных средств по дисциплине

Вопросы к экзамену

по дисциплине Кибербезопасность, цифровые риски и угрозы

1. Общие требования к организации, содержанию работ и результатамоказания услуг по ЗИ.
2. Классификация в области ЗИ (ОЗИ, угроз безопасности информации,уязвимостей ОЗИ, работ и услуг по ЗИ, техники ЗИ)
3. Требования к системе документов в области ЗИ и ССЗИ, в том числе требования к структуре системы документов, содержанию, оформлению, порядку разработки, согласования, утверждения и отмены
4. Общие технические требования по ЗИ, предъявляемые к различным ОЗИ
5. Общие требования к организации и содержанию работ по ЗИ на ОЗИ
6. Общие технические требования к СЗИ и СКЭЗИ и методам ихиспытаний
7. Методы контроля организации и эффективности ЗИ, методы измеренийпри проведении контроля
8. Общие требования к организации, содержанию работ и результатамоказания услуг по ЗИ.
9. Работа с высокоприоритетным трафиком - реализованным в АПКШКонтинент механизм приоритезации трафика.
10. Взаимодействие с системами управления сетью
11. Инвентаризация информационных систем и их критичности дляпредприятия
12. Управление уязвимостями —оценка текущего уровня уязвимостейего активов и текущий уровень их защиты.
13. Сбор данных об уязвимостях информационных систем
14. Сканирование сетевыми сканерами
15. Сбор информации о настройках, аппаратном и программномобеспечении
16. Проверка по базе данных уязвимостей
17. Доступ к информационной системе и настройки срзи:
18. .Настройки сетевых, так и встроенных в ОС firewall-ов
19. 11.Установив на актив антивирусное ПО или HIPS
20. 12.Настройки IPS системы, защищающей сегмент с активом
21. Заземление ОТСС и экранов их соединительных линий;
22. Звукоизоляция выделенных помещений.
23. Развязывание информационных сигналов:
24. Установка специальных средств защиты в ВТСС, обладающих "микрофонным эффектом" и имеющих выход за пределы контролируемой зоны;
25. Установка специальных диэлектрических вставок в оплетки кабелей электропитания, труб систем отопления, водоснабжения и канализации, имеющих выход за пределы контролируемой зоны;
26. Установка автономных или стабилизированных источников электропитания ОТСС;
27. Установка устройств гарантированного питания ОТСС (например, мотор-генераторов);
28. Установка в цепях электропитания ОТСС, а также в линиях осветительной и розеточной сетей выделенных помещенийпомехоподавляющих фильтров.
29. Симметричные криптосистемы и их свойства
30. Шифры замены
31. Шифры перестановки
32. Поточные криптосистемы
33. Блочные криптосистемы
34. Принципы построения блочных криптосистем
35. Режимы шифрования
36. Усложнение блочных криптосистем

37. Блочная криптосистема DES 41
38. Обобщенная схема асимметричной криптосистемы
39. Применение цифровой подписи
40. Сертификаты открытых ключей
41. Выдача сертификатов удостоверяющим центром CA
42. Типичная схема организации частной виртуальной сети сиспользованием VPN-шлюзов
43. Схема применения DSA-3110 в сети оператора
44. Схема применения DSA-3110 в сети компании
45. Хэш-функция, для чего она используется. В чём заключается устойчивость к столкновениям
46. Схемы хэширования с длиной хэш-значения, равнойдлине блока.
47. Схемы хэширования с длиной хэш-значения, равнойудвоенной длине блока.
48. Функции цифровая подпись. Основные свойства цифровой подписи.
49. Существующие схемы цифровой подписи. Самая распространенная схема.
50. Подпись RSA. Отличие подписи RSA от алгоритма шифрования RSA.
51. Подпись и проверка на подлинность подписи

Задачи к экзамену

Задача 1 Оцените защищенность компьютера вашего рабочего места от вирусов, вирусоподобных программ и сетевых атак путем исследования наличия программных средств и настроек. Дайте оценку полученным результатам

Задача 2 Оцените защищенность данных на компьютерах вашего сетевого окружения и серверах сети. Дайте оценку полученным результатам.

Задача 3 Оцените эффективность и безопасность работы компьютера вашего рабочего места с точки зрения наличия ошибок, ненужных файлов на диске и его фрагментации. Дайте оценку полученным результатам. Задача 4 Произведите оценку доступности компьютера вашего рабочего места для сетевых атак с точки зрения открытых для атак портов. Дайте оценку полученным результатам.

Задача 5 Произведите оценку открытости для сетевых атак заданного сайта. Узнайте его IP - адрес, владельца сайта, дату регистрацию домена, оплату домена, используемое ПО (CMS). Дайте оценку полученным результатам.

Задача 6 Произведите определение настроек браузера вашего компьютера, влияющих на безопасности работы в сети Интернет, а также актуальность браузера. Дайте оценку полученным результатам и рекомендации по улучшению настроек.

Задача 7 При включении компьютера, находящегося в корпоративной сети, вы обнаружили, что диск D не содержит информации, которая там была. Видимо, вирус сделал все объекты скрытыми. У вас нет прав администратора. Можно ли решить проблему без вызова инженера? Опишите ваши действия.

Задача 8 Пользователь заметил, что ПК стал выполнять операции, команды, которые им не отдавались, перезагружаться, «тормозить». Перечислите возможные причины. Составьте список действий, которые должен последовательно произвести пользователь.

Задача 9 Разрабатывается информационная система, которая, в том числе, должна обеспечить работу с персональными данными. Составьте список действий, которые необходимо выполнить на этапе проектирования системы, ее ввода в действие и при эксплуатации.

Задача 10 Разрабатывается информационная система, которая, в том числе, должна обеспечить работу с информацией ограниченного доступа (коммерческой тайной). Составьте список действий, которые необходимо выполнить на этапе проектирования системы, ее ввода в действие и при эксплуатации

Задача 11 Зашифруйте пословицу методом Цезаря и методом Гронсфельда. Открытый текст: ВСЁ ТАЙНОЕ СТАНОВИТСЯ ЯВНЫМ. Ключи назначьте сами. Оцените достоинства и недостатки использованных методов. Охарактеризуйте практическую значимость и сферу применения этих методов в настоящее время.

Задача 12. Пользователь получил сообщение от партнеров, зашифрованное. как сообщалось в письме, алгоритмом BlowFish, хэш Haval. Ранее пользователю был сообщен ключ. Как

расшифровать сообщение и послать ответное сообщение, зашифрованное таким же образом и с тем же ключем? Проиллюстрируйте действия на примере с ключем QWERTY. Зашифрованное сообщение:
bewdkbllvoJxe1laJmaqO1XMp5FvJeyrr5TV0OCzGvUNen6drkCOeiVeLbdstsUz5Pa9DJwI8FE
iqVUDWdNT21BBEv+b

Задача 13. Создайте папку Защищенная, а в ней несколько файлов. Средствами ОС зашифруйте созданную папку с файлами. выполните архивацию сертификата шифрования. Найдите способ снятия шифрования с папки и вложенных файлов. Оцените практическую пользу от такого шифрования.

Задача 14. На основе ГОСТ Р ИСО/МЭК 17799-2005, и с точки зрения начальника отдела по вопросам информационной безопасности в небольшой организации разработайте перечень мероприятий при привлечении сторонних организаций к обработке информации.

Задача 15. Приобретается новый компьютер с предустановленной проприетарной ОС. Составьте список последовательных мероприятий (действий) для обеспечения его эффективной и безопасной работы при введении в эксплуатацию.

Образец экзаменационного билета для промежуточной аттестации

СЕВЕРО-КАВКАЗСКАЯ ГОСУДАРСТВЕННАЯ АКАДЕМИЯ

Кафедра Прикладная информатика

20_ – 20_ уч. год

ЭКЗАМЕНАЦИОННЫЙ БИЛЕТ № 1

По дисциплине Кибербезопасность, цифровые риски и угрозы

Для обучающихся 4 курса направления подготовки 09.03.03 «Прикладная информатика»
Направленность (профиль) «Прикладная информатика в экономике»

Вопросы:

1. Управление уязвимостями —оценка текущего уровня уязвимостейего активов и текущий уровень их защиты.
2. Схемы хэширования с длиной хэш-значения, равнойдлине блока.
3. Создайте папку Защищенная, а в ней несколько файлов. Средствами ОС зашифруйте созданную папку с файлами. выполните архивацию сертификата шифрования. Найдите способ снятия шифрования с папки и вложенных файлов. Оцените практическую пользу от такого шифрования.

Зав. кафедрой Хапаева Л.Х.

Вопросы к устному опросу

по дисциплине Кибербезопасность, цифровые риски и угрозы

Вопросы к разделу 1.

1. Общие требования к организации, содержанию работ и результатамоказания услуг по ЗИ.
2. Классификация в области ЗИ (ОЗИ, угроз безопасности информации,уязвимостей ОЗИ, работ и услуг по ЗИ, техники ЗИ)
3. Требования к системе документов в области ЗИ и ССЗИ, в том числе требования к структуре системы документов, содержанию, оформлению, порядку разработки, согласования, утверждения и отмены
4. Общие технические требования по ЗИ, предъявляемые к различным ОЗИ
5. Общие требования к организации и содержанию работ по ЗИ на ОЗИ
6. Общие технические требования к СЗИ и СКЭЗИ и методам ихиспытаний
7. Методы контроля организации и эффективности ЗИ, методы измеренийпри проведении контроля
8. Общие требования к организации, содержанию работ и результатамоказания услуг по ЗИ.
9. Работа с высокоприоритетным трафиком - реализованным в АПКШКонтинент механизм приоритезации трафика.
10. Взаимодействие с системами управления сетью
11. Инвентаризация информационных систем и их критичности для предприятия
12. Управление уязвимостями —оценка текущего уровня уязвимостейего активов и текущий уровень их защиты.
13. Сбор данных об уязвимостях информационных систем
14. Сканирование сетевыми сканерами
15. Сбор информации о настройках, аппаратном и программномобеспечении
16. Проверка по базе данных уязвимостей

Вопросы к разделу 2.

1. Доступ к информационной системе и настройки срзи:
2. .Настройки сетевых, так и встроенных в ОС firewall-ов
3. 11.Установив на актив антивирусное ПО или HIPS
4. 12.Настройки IPS системы, защищающей сегмент с активом
5. Заземление ОТСС и экранов их соединительных линий;
6. Звукоизоляция выделенных помещений.
7. Развязывание информационных сигналов:
8. Установка специальных средств защиты в ВТСС, обладающих "микрофонным эффектом" и имеющих выход за пределы контролируемой зоны;
9. Установка специальных диэлектрических вставок в оплетки кабелей электропитания, труб систем отопления, водоснабжения и канализации, имеющих выход за пределы контролируемой зоны;
10. Установка автономных или стабилизированных источников электропитания ОТСС;
11. Установка устройств гарантированного питания ОТСС (например, мотор-генераторов);
12. Установка в цепях электропитания ОТСС, а также в линиях осветительной и розеточной сетей выделенных помещенийпомехоподавляющих фильтров.
13. Симметричные криптосистемы и их свойства
14. Шифры замены
15. Шифры перестановки
16. Поточные криптосистемы
17. Блочные криптосистемы

18. Принципы построения блочных криптосистем 34
19. Режимы шифрования
20. Усложнение блочных криптосистем
21. Блочная криптосистема DES 41
22. Обобщенная схема асимметричной криптосистемы
23. Применение цифровой подписи
24. Сертификаты открытых ключей
25. Выдача сертификатов удостоверяющим центром CA
26. Типичная схема организации частной виртуальной сети сиспользованием VPN-шлюзов
27. Схема применения DSA-3110 в сети оператора
28. Схема применения DSA-3110 в сети компании

Вопросы к разделу 3.

1. Хэш-функция, для чего она используется. В чём заключается устойчивость к столкновениям
2. Схемы хэширования с длиной хэш-значения, равнойдлине блока.
3. Схемы хэширования с длиной хэш-значения, равнойудвоенной длине блока.
4. Функции цифровая подпись. Основные свойства цифровой подписи.
5. Существующие схемы цифровой подписи. Самая распространенная схема.
6. Подпись RSA. Отличие подписи RSA от алгоритма шифрования RSA.
7. Подпись и проверка на подлинность подписи по алгоритму Эль-Гамаля.

Задания для контрольной работ

1. Совершенно стойкие криптосистемы
2. Идеально стойкие криптосистемы
3. Практическая стойкость криптосистем
4. Имитостойкость и помехоустойчивость криптосистем
5. Математические бэкдоры в алгоритмах шифрования
6. Линейный криптоанализ на примере блочного алгоритма шифрования NUSH
7. Блочная криптосистема ГОСТ 28147-89 43
8. Конкурс AES и блочная криптосистема Rijndael
9. Симметричные криптосистемы и их свойства
10. Шифры замены
11. Шифры перестановки
12. Поточные криптосистемы
13. Блочные криптосистемы
14. Принципы построения блочных криптосистем 34
15. Режимы шифрования
16. Усложнение блочных криптосистем
17. Блочная криптосистема DES 41

Задача 1. Произвести шифрование сообщения различными способами:

- шифром Цезаря;
- шифром многоалфавитной замены;
- с помощью квадрата Полибия;
- с помощью таблицы Виженера;
- методом перестановок;
- с помощью системы Плейфейра

Задача 2. Автоматическое устройство осуществило перекодировку информационного сообщения

на русском языке, первоначально записанного в 16-битном коде Unicode, в 8-битную кодировку КОИ-8. При этом информационное сообщение уменьшилось на 800 бит. Какова длина сообщения в символах?

Задача 3. Дешифрировать сообщение (шифр Цезаря)

Шифрограмма
1. ТСДЗЖЛХЗОЯОБДЛХТУЗЦЕЗОЛЪЛЕГХЯФЛОЦТСДЗИЖЗРРСЕС
2. ЪЗПШЦЙЗРСЕСФХЯХЗПДСОЯЫЗЛРЧСУПГЩЛЛСРГФСЖЗУЙЛХ
3. ТУГЕЛОГЖОВЕФЗШСЖЛРГНСЕЮЗХСОЯНСЛФНОБЪЗРЛВУГКРЮЗ
4. ЛКСДУЗХГХЗОВНСОЗФГСФСДЗРРСЪХВХДЗОНЛ
5. ДЗФТУЛРЩЛТРСФХЯАХСРЗСХФХЦХФХЕЛЗТУЛРЩЛТСЕГЛШЛКСДЛОЛЗ
6. НГНПГОССНУЮОЗРРЮШФУЗЖЛСНСОЯЩСЕГРРЮШ
7. НХСЕФЗЕЖГФЛЖЛХРГПЗОЛХСХРЛНСЕЖГРЗЦХСРЗХ
8. ХСХИЛЕЗХТУЛТЗЕГБЪЛНХСИЛЕЗХТСЖТЗЕГБЪЛ
9. ТУЗИЖЗЪЗПЕЮШСЖЛХЯЛКФЗДВСТУЗЖЗОЛХЗЖГОЯРЗМЫЛМПГУЫУЦХ
10. СУОЮФЛЖВХОЛДСРГЕЗУЫЛРЗОЛДСЕНОЗХНЗ
11. НСЕГОЯНСРВНЦЗГИГДГФЕСБРСЕЦФЦЗ
12. РГЦНЛДЮЕГБХЗФХЗФХЕЗРРЮПЛЛТУСХЛЕСЗФХЗФХЕЗРРЮПЛ
13. ВЛФГПЫЦХЛХЯРЗОБДОБЛОБЖВПРЗЖГП
14. ЗФОЛДГУЛРДЗКФГТСЕКРГЪЛХДГУЛРТЗЖГЕСЕ
15. ЛПЗББЬЛМЦЫЛЖГРЗСФХГРЗХФВДЗКОГТЫЛ
16. КГУВИЗРРСПЦХГРНЦЕЖЦОСРЗФПСХУВХ

Задача 4. Результатом шифрования слова «переставь» перестановкой по ключу «560832147» будет ...

- вертаепсь
- тапвсереь
- всерепьта
- тапьересв

Задача 5. Зашифровать свою фамилию и имя с помощью шифров:

- шифра «Перекресток»;
- шифры с использованием треугольника.

Тестовые вопросы

по дисциплине Кибербезопасность, цифровые риски и угрозы

ПК – 5

1.	Почему внутренние угрозы безопасности могут нанести организации еще больший ущерб, чем внешние?	1. Внутренние пользователи – более мастерские хакеры 2. Внутренние пользователи могут подключаться к инфраструктурным устройствам через Интернет 3. У внутренних пользователей прямой доступ к инфраструктурным устройствам 4. Внутренние пользователи могут получать доступ к корпоративным данным без аутентификации

2.	Как еще называют конфиденциальность информации?	1. Доверие 2. Согласованность 3. Неприкосновенность информации 4. Точность
3.	Какой способ используется для проверки целостности данных?	1. Резервная копия 2. Аутентификация 3. Контрольная сумма 4. Шифрование
4.	Какой тип атаки позволяет злоумышленнику воспользоваться методом подбора пароля (brute-force)?	1. Отказ в обслуживании 2. Перехват пакетов 3. Социальная инженерия 4. Взлом пароля
5.	Какой инструмент используется для получения списка открытых портов на сетевых устройствах?	1. Nmap 2. Tracert 3. Whois 4. Ping
6.	Для чего предназначен руткит?	1. Для доставки рекламы без согласия пользователя 2. Для саморепликации независимо от других программ 3. Для получения привилегированного доступа к устройствам без раскрытия себя 4. Для маскировки в качестве легитимной программы
7.	Если данные хранятся на локальном жестком диске, как лучше всего защитить их от неавторизованного доступа?	1. Двухфакторная аутентификация 2. Дублированная копия жесткого диска 3. Удаление конфиденциальных файлов 4. Шифрование данных
8.	Каким образом надежнее всего можно предотвратить использование уязвимости в Bluetooth?	1. Всегда использовать VPN при подключении с помощью Bluetooth 2. Использовать Bluetooth только при подключении к известному SSID 3. Всегда отключать Bluetooth, когда он активно не используется. 4. Использовать Bluetooth только для подключения к другому смартфону или планшету.
9.	Технология какого типа может предотвратить слежение вредоносным ПО за активностью пользователей, сбор персональной информации и выдачу нежелательной всплывающей рекламы на компьютере пользователя?	1. Менеджер паролей 2. Межсетевой экран 3. Антишпионское ПО 4. Двухфакторная аутентификация
10.	Какой тип атаки способен прерывать оказание услуг, переполняя сетевые устройства поддельным трафиком?	1. Сканирование портов 2. DDoS 3. Атака нулевого дня 4. Метод грубой силы
11.	Какой протокол используется решением по кибербезопасности Cisco Cyberthreat Defense для сбора информации о трафике, проходящем по сети?	1. HTTPS 2. Telnet 3. NetFlow 4. NAT

12.	Какой инструмент может выявлять вредоносный трафик, сравнивая содержимое пакета с известными сигнатурами атак?	1. NetFlow 2. Nmap 3. Zenmap 4. IDS

13. Термин «информация» определен как «сведения (сообщения, данные) независимо от формы их представления»:

1 Федеральным законом РФ N 149-ФЗ «Об информации, информационных технологиях и защите информации»

2 Постановлением Правительства РФ

14. Система обеспечения информационной безопасности информации должна базироваться на следующих принципах:

1 непрерывность
2 комплексность
3 системность
4 законность

15. По физической природе технические каналы утечки информации подразделяются на:

1 оптические
2 акустические
3 радиоэлектронные
4 химические

16.К косвенным каналам утечки информации относятся:

1 кража или утеря носителей информации
2 исследование не уничтоженного мусора
3. перехват электромагнитных излучений
4. копирование информации

17 Сертификат ЭЦП – это:

1 электронный документ, содержащий открытый ключ ЭЦП пользователя
2 бумажный документ, содержащий открытый ключ ЭЦП пользователя

18. Выберите категорию, к которой относятся персональные данные, позволяющие идентифицировать субъекта персональных данных:

1. 7 категория
2. 3 категория
3. 5 категория

19. Вставьте пропущенное слово:

Субъектом персональных данных является … лицо.

20 Следующие методы инженерно-технической защиты информации используются для противодействия подслушиванию:

1 использование отдельного входа 2 энергетическое скрытие
3 обнаружение и выведение из строя закладных устройств 4 повышение звукопоглощения

21. Выберите, что из перечисленного не относится к возможным угрозам информационной безопасности:

1 компьютерные преступления на основе ложной идентификации клиента 2 подделка электронных документов
3 получение злоумышленником конфиденциальной информации 4 кажущаяся анонимность при

работе в Internet

22. Система защиты информации определяется:
1 как организованную совокупность специальных органов, средств, методов и мероприятий, обеспечивающих защиту информации от внутренних и внешних угроз
2 как совокупность информационной инфраструктуры, субъектов, осуществляющих сбор, формирование, распространение и использование информации, а также системы регулирования возникающих при этом общественных отношений
3 как одно из наиболее общих понятий науки, обозначающее некоторые сведения, совокупность каких-либо данных, знаний и т. п.

23. Укажите, какой вид собственного обеспечения системы защиты информации предполагает широкое использование технических средств как для защиты информации, так и для обеспечения деятельности собственно средств защиты информации:
1 лингвистическое обеспечение
2 организационное обеспечение
3 аппаратное обеспечение

24. Укажите, какой вид собственного обеспечения системы защиты информации включает в себя сведения, данные, показатели, параметры, лежащие в основе решения задач, обеспечивающих функционирование системы:
1 аппаратное обеспечение
2 организационное обеспечение
3 информационное обеспечение
4 правовое обеспечение

25. Под утечкой информации понимается:
1 процесс уничтожения информации
2 непреднамеренная утрата носителя информации
3 несанкционированный процесс переноса информации от источника к злоумышленнику

26. Какой тип взломщиков интрасетей, согласно одной из классификаций компьютерных злоумышленников, отличается от других типов тем, что после входа в систему он должен найти и перенести определенную информацию на свой компьютер, что делает его задачу более сложной, чем простое проникновение:
1 «луддит»
2 «хулиган»
3 «шпион»

27. Укажите, что является основным правовым документом, определяющим защищенность предприятия от внутренних и внешних угроз:
1 концепция современных информационных технологий
2 концепция безопасности информации
3 концепция информационных ресурсов

28. Какая причина уязвимости Интернет сформулирована неверно:
1 работа в Internet обслуживается большим числом сервисов, информационных служб и сетевых протоколов, знание правильности и тонкостей использования всех или хотя бы большинства сервисов, служб и протоколов одному человеку в лице администратора сети нереально;

2 «утечка» технологий высокого уровня из секретных источников при вскрытии представленных в сети Web-узлов и сетей организаций, занимающихся разработкой этих технологий, и доступность информации о средствах защиты;

3 зашифрованность большей части передаваемой через Internet информации

29. Целью какого организационного мероприятия является исключение возможности тайного проникновения на территорию и в помещения посторонних лиц и обеспечение удобства контроля прохода и перемещения сотрудников и посетителей:
1 организации работы по анализу внутренних и внешних угроз 2 организации работы с документами
3 организации работы с сотрудниками
4 организации использования технических средств 5 организации режима и охраны

30. Назовите виды электронной цифровой подписи определены в ФЗ «Об электронной подписи»

31. Вставьте пропущенное слово:
Документированная информация, доступ к которой ограничивается в соответствии с законодательством РФ называется …

32. Согласно каким методам шифрования информации, шифрование выполняется путем сложения символов исходного текста и ключа по модулю, равному числу букв в алфавите:
1 аддитивным методам
2 методам перестановки
3 методам замены (подстановки)

33. Как называется детектирование вируса в незараженном объекте (файле, секторе или системной памяти)

34. Укажите, как называется комплекс мероприятий, исключающих или уменьшающих возможность выхода конфиденциальной информации за пределы контролируемой зоны за счет акустических полей

35. Назовите стандартСтандарты появлялись, развивались и угасали: RPC, CORBA, DCOM, RMI…, последним в этом ряду стал протокол SOAP, основа современных Web-сервисов

Задания для лабораторных работ

по дисциплине Кибербезопасность, цифровые риски и угрозы

Лабораторная работа №1
Сравнение данных с помощью хэш-функции

Цель работы: использовать программу хэширования для проверки целостности данных.
1. Создание текстового файла
2. Установка HashCalc
3. Вычисление хэш файла Hash.txt

Лабораторная работа №2. Создание и сохранение надежных паролей

Цель работы: понять, что такое надежный пароль.
1. Понятие надежного пароля
2. Создание надежного пароля.

Лабораторная работа №3.
Резервное копирование данных во внешнее хранилище

Цель работы: создать резервную копию данных пользователя.

1. Использование локального внешнего диска для резервного копирования данных
2. Использование удаленного диска для резервного копирования данных

Лабораторная работа №4.
Организация защиты рабочих станций и информационных систем, в соответствии с требованиями национальных стандартов

Цель лабораторной работы – приобрести практические умения использования прикладного программного обеспечения в целях защиты рабочих станций и информационных систем, в соответствии стребованиями национальных стандартов.

Примерные варианты заданий

Построить модель угроз ИСПДн Вашего предприятия. Для построения модели угроз необходимо проработать теоретический материал лабораторной работы и заполнить таблицу 1.

Таблица 1 – Характеристики для определения исходного уровнязащищённости ИСПДн

По территориальному размещению			
распределенная ИСПДн, которая охватывает несколько областей, краев, округов или государство в целом			
городская ИСПДн, охватывающая не более одного населенного пункта (города, поселка)			
корпоративная распределенная ИСПДн, охватывающая многие подразделения одной организации			
локальная (кампусная) ИСПДн, развернутая в пределах нескольких близко расположенных зданий;			
локальная ИСПДн, развернутая в пределах одного здания			
По наличию соединения с сетями общего пользования			
ИСПДн, имеющая многоточечный выход в сеть общего пользования;			
ИСПДн, имеющая одноточечный выход в сеть общего пользования;			
ИСПДн, физически отделенная от сети общего пользования			
По встроенным (легальным) операциям с записями баз персональных данных			
чтение, поиск;			
запись, удаление, сортировка;			
модификация, передача			
По разграничению доступа к персональным данным			
ИСПДн, к которой имеют доступ определенные перечнем сотрудники организации, являющейся владельцем ИСПДн, либо субъект ПДн;			
ИСПДн, к которой имеют доступ все сотрудники организации, являющейся владельцем ИСПДн;			
ИСПДн с открытым доступом			
По наличию соединений с другими базами ПДн иных ИСПДн			
интегрированная ИСПДн (организация использует несколько баз ПДн ИСПДн, при этом организация не является владельцем всех используемых баз ПДн);			
ИСПДн, в которой используется одна база ПДн, принадлежащая организации – владельцу данной ИСПДн			
По уровню обобщения (обезличивания) ПДн			
ИСПДн, в которой предоставляемые пользователю данные являются обезличенными (на уровне организации, отрасли, области,			

Лабораторная работа №5.
Настройка функционала защиты информации при эксплуатации программно-аппаратных комплексов.

Цель лабораторной работы – приобрести практические навыки интеграции и настройки функционала защиты информации приэксплуатации программно-аппаратных комплексов

Примерные варианты заданий

В данных Рекомендациях предлагается использовать поэтапныйподход к построению системы

защиты информации:
Этап 1 позволяет понять, что находится в вашей сети, и определяетбазовые требования по информационной безопасности;
Этап 2 уделяет основное внимание обеспечению базовыхтребований безопасности и обучению сотрудников вопросам информационной безопасности.
Этап 3 помогает вашей организации подготовиться к инцидентам по информационной безопасности.
На каждом этапе вам будут представлены вопросы, на которые необходимо ответить, а также действия и инструменты, которые помогут достичь ваших целей.

Лабораторная работа №6.
Способы защиты от утечки информации по техническим каналам.

Цель лабораторной работы – приобрести практические умения использования ресурсов программно-аппаратных комплексов в вопросах защиты информации

Примерные варианты заданий

Первая часть работы проводится с применением генератора шума, установленного в свободный слот персонального компьютера, и компьютеризированного комплекса
Для этого:
1) Снять частотную панораму в помещении с помощью комплекса при выключенном генераторе шума.
2) Снять частотную панораму при включенном генераторе шума.
Путем сравнения частотных панорам оценить эффективность маскировки электромагнитных излучений персонального компьютера и других находящихся в помещении электронных устройств с помощьюгенератора шума.
Вторая часть работы проводится с демонстрацией действия устройств.
С этой целью:
1. Поочередно включить каждое из устройств и делаются попытаться
установить связь с любым абонентом по сотовому телефону.
5) Для наблюдения сигналов зашумления использовать комплекс.
6) Составить отчет с описанием способов маскировки электромагнитных излучений средств вычислительной техники иустройств и ответить на контрольные вопросы.

Лабораторная работа №7.
Защита графического файла с помощью цифрового водяного знака с применением LSB алгоритма.

Цель работы: Изучение стеганографических методов защиты информации. Реализация программы с использованиемстеганографических принципов защиты информации.
Практическое задание
1. Разработать собственное приложение, в котором должен бытьреализован метод НЗБ. При этом:
- выбор файла-контейнера – по согласованию с преподавателем;
- реализовать два варианта осаждаемого/извлекаемого сообщения:

− собственные фамилия, имя и отчество;
− текстовая часть отчета по одной из выполненных лабораторных работ;

- реализовать два метода (на собственный выбор) размещения битового потока осаждаемого сообщения по содержимому контейнера;
- сформировать цветовые матриц, отображающие каждый задействованный для осаждения уровеньмладших значащих битов контейнера;
- выполнить визуальный анализ (с привлечением коллег в качестве экспертов) стеганоконтейнеров с различным внутренним содержанием; сделать выводы на основе

выполненного анализа.

2. Результаты выполнения работы оформить в виде отчета по установленным правилам

Контрольные вопросы

1. Охарактеризовать цели, задачи и области применениястеганографии.
2. В чем состоят сходства и различия между стеганографией икриптографией?
3. Дать определение стеганографической системы. Охарактеризовать составные части стеганосистемы и их взаимосвязь.
4. Основные классификационные критерии методов стеганографии.
5. Пояснить сущность основных атак на стеганосистемы.
6. Изобразить структурную схему стеганографической системы.
7. Сущность метода НЗБ. Области его применении.
8. Изобразить алгоритмы встраивания и извлечения сообщений на основе метода НЗБ при передаче этих сообщений.
9. Изобразить алгоритмы встраивания и извлечения сообщений на основе метода НЗБ при решении задачи защиты прав интеллектуальной собственности на электронный контент.

Лабораторная работа №8.
Метод Куттера-Джордана-Боссена

Цель лабораторной работы: изучить метод Куттера-Джордана- Боссена, приобрести практические умения скрытия информации в изображениях.

Разработать собственное приложение, в котором должен быть реализован метод Куттера-Джордана-Боссена. При этом:

- выбор файла-контейнера – по согласованию с преподавателем;
- реализовать два варианта осаждаемого/извлекаемого сообщения:

− собственные фамилия, имя и отчество;

− текстовая часть отчета по одной из выполненных лабораторных работ;

- выполнить визуальный анализ (с привлечением коллег в качестве экспертов) стеганоконтейнеров с различным внутренним содержанием; сделать выводы на основе выполненного анализа.

Результаты выполнения работы оформить в виде отчета по установленным правилам

Лабораторная работа №9.
Симметричные криптосистемы шифрования.

Цель лабораторной работы – изучение использования методов симметричного шифрования при передаче информации с целью защиты данных

Примерные варианты заданий

Реализовать приложение для шифрования, позволяющее выполнять следующие действия:

1. Шифровать данные по заданному в варианте алгоритму:

1) шифруемый текст должен храниться в одном файле, а ключ шифрования – в другом;
2) зашифрованный текст должен сохраняться в файл;
3) в процессе шифрования предусмотреть возможность просмотра и изменения ключа, шифруемого и зашифрованного текстов вшестнадцатеричном и символьном виде;
4) программа должна показывать время шифрования.

2. Исследовать лавинный эффект (исследования проводить на одном блоке текста):

1) для бита, который будет изменяться, приложение должнопозволять задавать его позицию (номер) в открытом тексте или в ключе;
2) приложение должно уметь после каждого раунда шифрования подсчитывать число бит, изменившихся в зашифрованном тексте при изменении одного бита в открытом тексте либо в ключе;
3) приложение может строить графики зависимости числа бит, изменившихся в зашифрованном тексте, от раунда шифрования, либо графики можно строить в стороннем ПО, но тогда

приложение для шифрования должно сохранять в файл необходимую для построения графиков информацию. II. Реализовать приложение для дешифрования, позволяющее выполнять следующие действия:

3. Дешифровать данные по заданному в варианте алгоритму:

1) зашифрованный текст должен храниться в одном файле, ключ – вдругом;

2) расшифрованный текст должен сохраняться в файл;

3) в процессе дешифрования предусмотреть возможность просмотра и изменения ключа, зашифрованного и расшифрованного текстов в шестнадцатеричном и символьном виде.

Реализовать приложение, вычисляющее значения 1–4 критериев дляалгоритмов DES и ГОСТ. Можно взять стороннюю реализацию того алгоритма, который не указан в варианте.

4. С помощью реализованных приложений выполнить следующие задания:

1. Протестировать правильность работы разработанных приложений.

2. Исследовать лавинный эффект при изменении одного бита в открытом тексте и в ключе: построить графики зависимостей числа бит, изменившихся в зашифрованном сообщении, от раунда шифрования (всего должно быть построено 2 графика).

3. Сравнить значения критериев 1–4 для алгоритмов DES и ГОСТ при изменении одного бита в блоке открытого текста и одного бита в ключе при использовании одного и того же сообщения. Сообщение должно состоять хотя бы из пяти блоков (чем больше, тем точнее будут оценки критериев 1–4).

4. Сделать выводы о проделанной работе.

Лабораторная работа №10.
Асимметричные криптосистемы шифрования.

Цель лабораторной работы – изучение использования методов асимметричного шифрования при передаче информации с целью защиты данных

Примерные варианты заданий

Результатом данной лабораторной работы должны стать приложения, совмещающие в себе достоинства симметричных и асимметричных методов шифрования.

Реализовать приложение для шифрования, позволяющеевыполнять следующие действия:

1. Вычислять открытый и закрытый ключи для алгоритма RSA:

1) числа и генерируются программой или задаются из файла;

2) числа и должны быть больше, чем;

3) сгенерированные ключи сохраняются в файлы: открытый ключ () – в один файл, закрытый ( ) – в другой.

Шифровать указанным в варианте симметричным алгоритмомоткрытый текст, а асимметричным – ключ симметричного алгоритма:

1) шифруемый текст должен храниться в одном файле, открытый ключ ( ) для алгоритма RSA – в другом;

2) ключ для симметричного алгоритма должен генерироваться случайным образом;

3) зашифрованный текст должен сохраняться в одном файле, а зашифрованный асимметричным алгоритмом ключ симметричногоалгоритма – в другом;

4) в процессе шифрования предусмотреть возможность просмотра иизменения шифруемого текста в шестнадцатеричном и символьном виде;

5) программа должна уметь работать с текстом произвольной длины. II. Реализовать приложение для дешифрования.

1. Зашифрованный текст должен храниться в одном файле, зашифрованный ключ симметричного алгоритма – в другом, а секретный ключ для алгоритма RSA – в третьем. 3

2. Приложение расшифровывает зашифрованный ключ с помощью алгоритма RSA, а затем с помощью симметричного алгоритма с ключом расшифровывает зашифрованный текст.

3. Расшифрованный текст должен сохраняться в файл.

4. В процессе дешифрования предусмотреть возможность просмотра и изменения

зашифрованного текста в шестнадцатеричном и символьном виде.

5. Программа должна уметь работать с текстом произвольной длины.

Лабораторная работа №11. Электронная цифровая подпись.

Цель лабораторной работы – исследование алгоритма создания ЭЦП для подписания электронных документов

Примерные варианты заданий

Реализовать приложение, позволяющее вычислять и проверять ЭЦП, сформированную по алгоритмам RSA и Эль-Гамаля.

Для построения подписи Эль-Гамаля следует использовать открытые параметры.

Вариант	ЭЦП по алгоритму RSA		ЭЦП по алгоритму Эль-Гамаля	
	Открытые ключи	Проверяемые сообщения $\langle m, s\rangle$, где m – хэш-значение сообщения M	Секретные параметры	m – хэш сообщения M
1	$n = 55,\ e = 3$	$\langle 7, 28\rangle,\ \langle 22, 15\rangle,\ \langle 16, 36\rangle$	$x = 11,\ k = 3$	$m = 15$
2	$n = 65,\ e = 5$	$\langle 10, 30\rangle,\ \langle 6, 42\rangle,\ \langle 6, 41\rangle$	$x = 10,\ k = 15$	$m = 5$
3	$n = 77,\ e = 7$	$\langle 13, 41\rangle,\ \langle 11, 28\rangle,\ \langle 5, 26\rangle$	$x = 3,\ k = 13$	$m = 8$
4	$n = 91,\ e = 5$	$\langle 15, 71\rangle,\ \langle 11, 46\rangle,\ \langle 16, 74\rangle$	$x = 18,\ k = 7$	$m = 16$
5	$n = 33,\ e = 3$	$\langle 17, 8\rangle,\ \langle 10, 14\rangle,\ \langle 24, 18\rangle$	$x = 9,\ k = 19$	$m = 3$
6	$n = 143,\ e = 37$	$\langle 46, 85\rangle,\ \langle 16, 74\rangle,\ \langle 129, 116\rangle$	$x = 19,\ k = 5$	$m = 11$
7	$n = 221,\ e = 43$	$\langle 59, 19\rangle,\ \langle 79, 164\rangle,\ \langle 58, 20\rangle$	$x = 14,\ k = 17$	$m = 14$
8	$n = 85,\ e = 15$	$\langle 24, 39\rangle,\ \langle 39, 51\rangle,\ \langle 83, 42\rangle$	$x = 6,\ k = 13$	$m = 9$
9	$n = 187,\ e = 77$	$\langle 139, 90\rangle,\ \langle 62, 163\rangle,\ \langle 95, 57\rangle$	$x = 4,\ k = 3$	$m = 4$
10	$n = 221,\ e = 79$	$\langle 207, 142\rangle,\ \langle 112, 9\rangle,\ \langle 82, 147\rangle$	$x = 15,\ k = 15$	$m = 17$
11	$n = 57,\ e = 31$	$\langle 25, 28\rangle,\ \langle 12, 42\rangle,\ \langle 48, 15\rangle$	$x = 12,\ k = 13$	$m = 18$
12	$n = 133,\ e = 41$	$\langle 52, 89\rangle,\ \langle 82, 120\rangle,\ \langle 67, 128\rangle$	$x = 7,\ k = 7$	$m = 12$
13	$n = 209,\ e = 67$	$\langle 49, 125\rangle,\ \langle 105, 17\rangle,\ \langle 136, 97\rangle$	$x = 13,\ k = 19$	$m = 20$

5. Методические материалы, определяющие процедуры оцениваниякомпетенции

5.1 Критерии оценивания качества устного ответа

Оценка **«отлично»** выставляется за глубокое знание предусмотренного программой материала, за умение четко, лаконично и логически последовательно отвечать на поставленные вопросы.

Оценка **«хорошо»** – за твердое знание основного (программного) материала, заграмотные, без существенных неточностей ответы на поставленные вопросы.

Оценка **«удовлетворительно»** – за общее знание только основного материала, за ответы, содержащие неточности или слабо аргументированные, с нарушением последовательности изложения материала.

Оценка **«неудовлетворительно»** – за незнание значительной части программного материала, за существенные ошибки в ответах на вопросы, за неумение ориентироваться в материале, за незнание основных понятий дисциплины.

5.2 Критерии оценивания тестирования

При тестировании все верные ответы берутся за 100%.90%-100% отлично
75%-90% хорошо
60%-75% удовлетворительно
менее 60% неудовлетворительно

5.3 Критерии оценивания качества выполнения лабораторных работ

Оценка **«зачтено»** выставляется обучающемуся, если лабораторная работа выполнена правильно и студент ответил на все вопросы, поставленные преподавателем на защите.

Оценка **«не зачтено»** выставляется обучающемуся, если лабораторная работа выполнена не правильно или студент не проявил глубоких теоретических знаний при защите работы

5.4 Критерии оценивания результатов освоения дисциплины на экзамене

Оценка **«отлично»** выставляется за глубокое знание предусмотренного программой материала, содержащегося в основных и дополнительных рекомендованных литературных источниках, за умение четко, лаконично и логически последовательно отвечать на поставленные вопросы, за умение анализировать изучаемые явления в их взаимосвязи и диалектическом развитии, применять теоретические положения при решении практических задач.

Оценка **«хорошо»** – за твердое знание основного (программного) материала, включая расчеты (при необходимости), за грамотные, без существенных неточностей ответы на поставленные вопросы, за умение применять теоретические положения для решенияпрактических задач.

Оценка **«удовлетворительно»** – за общее знание только основного материала, за ответы, содержащие неточности или слабо аргументированные, с нарушением последовательности изложения материала, за слабое применение теоретических положений при решении практических задач.

Оценка **«неудовлетворительно»** – за незнание значительной части программного материала, за существенные ошибки в ответах на вопросы, за неумение ориентироваться в расчетах, за незнание основных понятий дисциплины.

5.5 Критерии оценивания выполнения контрольной работы

Оценка **«отлично»** выставляется при условии, что обучающийся полностью выполнил задание контрольной и проявил отличные знания учебного материала. При этом работа оформлена в соответствии с требованиями и ГОСТом, к ней можно предъявить минимум замечаний.

Оценка **«хорошо»** ставится тогда, когда обучающийся выполнил все задания, показал хорошие знания по пройденному материалу, но не сумел обосновать предложенные решения задач, когда есть недочеты в оформлении контрольной работы и общие небольшие замечания, не влияющие на ее качество.

Оценку **«удовлетворительно»** обучающийся получает за полностью выполненное задание контрольной при наличии в ней существенных неточностей и недочетов, не умении

обучающимся верно применить полученные знания, в оформлении работы есть нарушения ГОСТ, не аргументированные ответы, неактуальные или ненадежные источники информации.
Оценку **«неудовлетворительно»** обучающийся получает в том случае, когда он не полностью выполнил задание, проявил недостаточный уровень знаний, не смог объяснить полученные результаты. Такая контрольная работа не отвечает требованиям, содержит противоречивые сведения, задачи в ней решены неверно.

30