МИНИСТЕРСТВО НАУКИ И ВЫСШЕГО ОБРАЗОВАНИЯ РОССИЙСКОЙ ФЕДЕРАЦИИ

Федеральное государственное автономное образовательное учреждение
высшего образования
«Национальный исследовательский технологический университет «МИСиС»
Институт информационных технологий и автоматизированных систем управления

КАФЕДРА ЭиИИС

СОГЛАСОВАНО:

Начальник Учебно-методического
управления
_____ А.А. Волков

«____» _____ 2020 г.

ПРИНЯТА:

на заседании Ученого совета института ИТАСУ
_____ С.В. Солодов

«____» _____ 2020 г.

ДОПОЛНИТЕЛЬНАЯ ПРОФЕССИОНАЛЬНАЯ ПРОГРАММА
(повышение квалификации)

Кибербезопасность

Автор курса:

Бахаров Л.Е.,
Старший преподаватель кафедры ЭиИИС

Москва, 2020

Раздел 1 Характеристика программы

1.1 Цель реализации программы: совершенствование профессиональных компетенций обучающихся в области кибербезопасности.

Совершенствуемые компетенции

№ п/п	Компетенции	Направление подготовки 44.03.01 Педагогическое Образование
		Бакалавриат
		Код компетенции
1.	Способен осуществлять педагогическую деятельность на основе специальных научных знаний	ОПК-8

1.2 Планируемые результаты обучения

№ п/п	Уметь – знать	Направление подготовки 44.03.01 Педагогическое Образование
		Бакалавриат
		Код компетенции
1.	**Введение в кибербезопасность**	
1.1	**Уметь:** определять длину пароля и вероятность его подбора при заданных параметрах системы аутентификации; **Знать:** - основные понятия и определения в области кибербезопасности; - классификацию и свойства информации; - угрозы информации и их классификация; - действия, приводящие к незаконному овладению информацией; - алгоритм определения длины пароля и вероятность его подбора при заданных параметрах системы аутентификации.	ОПК – 8
1.2	**Уметь:** - анализировать возможные действия злоумышленников по проникновению в локальную сеть организации с применением технологий социальной инженерии; - формулировать рекомендации для построения политики безопасности в части противодействия социальной инженерии. **Знать:** - определение социальной инженерии; - технологии социальной инженерии в информационном противоборстве; - типовые решения защиты от утечки конфиденциальной информации;	ОПК – 8

	– стратегии противодействия технологиям социальной инженерии**.**	
2	**Математические методы обеспечения кибербезопасности**	
2.1	**Уметь:** осуществлять шифрование текстового файла с помощью специального программного обеспечения различными методами и сравнивать их криптостойкость. **Знать:** - оопределения и концепции криптографии; - принципы Керкхофса; - факторы, определяющие стойкость криптосистем; - ссервисы, предоставляемые криптосистемами; - принцип действия одноразового шифровального блокнота; - классические криптоалгоритмы шифры подстановки и перестановки; – алгоритм шифрования текстового файла с помощью специального программного обеспечения различными методами и сравнения их криптостойкости.	ОПК – 8
2.2	**Уметь:** осуществлять один цикл шифрования текста с применением ГОСТ 28147-89 в режиме простой замены **Знать:** - преимущества и недостатки симметричных и ассиметричных криптостистем; - принципы построения блочных и потоковых шифров; - гибридные методы шифрования и технологию цифрового конверта; - принцип работы современных симметричных криптостистем на примере алгоритма шифрования ГОСТ 28147-89.	ОПК – 8
2.3	**Уметь:** зашифровать и расшифровать заданное сообщение с помощью алгоритмов RSA, Меркля-Хеллмана и Эль-Гамаля. **Знать:** - алгоритмы Диффи-Хеллмана, RSA, ELGAMAL, Меркля-Хеллмана и Эль-Гамаля; - принцип работы криптоалгоритмов, основанных на эллиптических кривых; - алгоритмы, основанные на «последовательностях Люка»; - принцип работы ранцевой криптосистемы; - протокол доказательства с нулевым разглашением.	ОПК – 8
2.4	**Уметь:** вычислять с помощью алгоритма MD5 хэш от заданного сообщения. **Знать:**	ОПК – 8

	- определение хэш-функций, их виды и способы построения; - схемы безопасного хэширования; - коллизии хэш-функций и их виды; - методы поиска коллизий; - примеры современных алгоритмов хэширования.	
2.5	**Уметь:** формировать и проверять подписи к заданному сообщению по алгоритмам RSA, ELGAMAL и DSA **Знать:** - понятие аутентификации данных и цифровая подпись; - алгоритмы цифровой подписи; - меры по защите от подделки цифровых подписей; - способы управление ключами цифровых подписей; - алгоритмы формирования и проверки цифровой подписи к заданному сообщению по алгоритмам RSA, ELGAMAL и DSA.	ОПК – 8
2.6	**Уметь:** производить встраивание заданной информации в программный файл и ее последующее извлечение с помощью специального программного обеспечения **Знать:** - определение и основные понятия стеганографии; - историю развития стеганографии как науки; - основные требования к стегосистемам; - виды контейнеров с стегосистемам и требования к ним; - применение стеганографии в кибербезопасности; - алгоритмы встраивания информации в мультимедийные файлы и в программное обеспечение и ее последующее извлечение.	ОПК – 8
3.	**Противодействие вредоносному программному обеспечению**	
3.1	**Уметь:** определять тип заданных описанием программ по классификации лаборатории Касперского. **Знать:** - алгоритм определения типа заданных описанием программ по классификации лаборатории Касперского; - общее определение компьютерного вируса; - разновидности вирусов, их свойства и способы противодействия распространению; - типичные симптомы вирусной атаки; - черви: определение, свойства и способы противодействия распространению; - логические бомбы и их особенности; - троянские объекты: определение, свойства и способы противодействия распространению; - программы backdoor и их особенности; - разновидности и опасность шпионского программного обеспечения; - разновидности и опасность программ adware.	ОПК – 8
3.2	**Уметь:**	ОПК – 8

	выполнять проверку работы антивирусных программ с помощью тестовых вирусов. **Знать:** - алгоритм проверки работы антивирусных программ с помощью тестовых вирусов; - принципы построения систем антивирусной защиты; - требования к антивирусным пакетам; - состав антивирусного пакета; - основные методы антивирусной защиты.	
3.3	**Уметь:** разрабатывать учебные занятия о сетевых атаках и способах противодействия им. **Знать:** - виды наиболее распространенных сетевых атак; - определение сетевого экрана и его основные задачи; - режимы работы сетевого экрана; - критерии качества работы сетевого экрана; - утечки, базовые идеи и технологии, позволяющие обойти защиту сетевого экрана; - алгоритм разработки учебного занятия о сетевых атаках и способах противодействия им.	ОПК – 8

1.3 Категория обучающихся. Уровень образования – высшее образование, область профессиональной деятельности – обучение информатике на уровне среднего общего образования в общеобразовательной организации.

1.4 Форма обучения – очная.

1.5 Трудоемкость программы, режим занятий – всего 72 часа, в том числе 48 часов аудиторной работы, включая итоговую аттестацию, 24 часа самостоятельной работы слушателей.

Раздел 2. *«Содержание программы»*

2.1. Учебный (тематический) план

№ п/п	Наименование разделов (модулей) и тем	Аудиторные учебные занятий, учебные работы			Внеаудиторная работа	Формы контроля	трудоемкость
		Всего ауд., час	Лекции	Практические занятия	с/р		
1	**Раздел 1. Введение в кибербезопасность**						
1.1.	Основные понятия кибербезопасности	4	2	2	1	Практическое задание № 1	5
1.2.	Социальная инженерия и кибербезопасность	4	2	2	1	Решение кейсов № 1	5

2	**Раздел 2. Математические методы обеспечения кибербезопасности**						
2.1.	Введение в криптографию	4	2	2	2	Практическое задание № 2	6
2.2.	Симметричные криптосистемы	4	2	2	2	Практическое задание № 3	6
2.3.	Криптосистемы с открытым ключом	6	4	2	2	Практическое задание № 4	8
2.4.	Хэш-функции в криптографии	4	2	2	2	Практическое задание № 5	6
2.5.	Цифровая подпись	4	2	2	2	Практическое задание № 6	6
2.6.	Стеганография	4	2	2	2	Практическое задание № 7	6
3	**Раздел 3. Противодействие вредоносному программному обеспечению**						
3.1.	Вредоносное программное обеспечение	4	2	2	2	Решение кейсов № 2	6
3.2.	Системы антивирусной защиты	4	2	2	2	Практическое задание № 8	6
3.3.	Сетевые экраны	5	2	3	6	Проект № 1	11
	Итоговая аттестация	1		1		Зачет на основании совокупности выполненных работ+результаты итогового тестирования	1
	Итого:	48			24		72

2.2. Учебная программа

№ п/п	Виды учебных занятий, учебных работ	Содержание
Раздел 1. Введение в кибербезопасность		
Тема 1.1 Основные понятия кибербезопасности	*Лекция (2 час.)*	Кибербезопасность как составная часть информационной безопасности. Основные понятия и определения в области кибербезопасности. Классификация и свойства информации. Угрозы информации и их классификация. Действия, приводящие к незаконному овладению информацией. Алгоритм определения длины пароля и вероятность его подбора при заданных параметрах системы аутентификации

	Практическое занятие (2 час.)	**Практическое задание № 1**. Расчет параметров парольной аутентификации. Определить длину пароля и вероятность его подбора при заданных параметрах системы аутентификации.
	Самостоятельная работа (1 час)	**Практическое задание № 1** Определение длины пароля и вероятность его подбора при заданных параметрах системы аутентификации. Подготовка и отправка отчета о проделанной работе.
Тема 1.2 Социальная инженерия и кибербезопасность	*Лекция (2 час.)*	Определение социальной инженерии. Технологии социальной инженерии в информационном противоборстве. Метод прямого воздействия. Метод введения в заблуждение. Метод обратной инженерии. Метод сбора и анализа информации из открытых источников. Типовые решения защиты от утечки конфиденциальной информации. Стратегии противодействия технологиям социальной инженерии.
	Практическое занятие (2 час.)	**Решение кейсов № 1** Деловая игра «Противодействие социальной инженерии». Разбиться на команды по 4-5 человек. Проанализировать возможные действия злоумышленников по проникновению в локальную сеть организации с применением технологий социальной инженерии. **Практическое задание № 2.** Используя сценарий другой команды, сформулировать рекомендации для построения политики безопасности в части противодействия социальной инженерии.
	Самостоятельная работа (1 час)	**Практическое задание № 2.** В заданных условиях проанализировать возможные действия злоумышленников по проникновению в локальную сеть организации с применением технологий социальной инженерии. Сформулировать рекомендации для построения политики безопасности в части противодействия социальной инженерии. Подготовка и отправка отчета о проделанной работе.
Раздел 2. Математические методы обеспечения кибербезопасности.		
Тема 2.1 Введение в криптографию	*Лекция (2 час.)*	История криптографии. Определения и концепции криптографии. Принципы Керкхофса. Стойкость криптосистем их факторы. Сервисы криптосистем. Одноразовый шифровальный блокнот и принцип его действия. Классические криптоалгоритмы подстановки и перестановки для защиты текстовой информации. Алгоритм шифрования текстового файла с помощью специального программного обеспечения различными методами и сравнения их криптостойкости

	Практическое занятие (2 час.)	**Практическое задание № 2.** Использование классических криптоалгоритмов подстановки и перестановки для защиты текстовой информации. Изучить на практике шифры подстановки и перестановки с применением частотного анализа. Зашифровать текстовый файл различными методами и сравнить их криптостойкость.
	Самостоятельная работа (2 час.)	**Практическое задание № 2.** Зашифровать текстовые файлы различными методами и сравнить их криптостойкость. Подготовка и отправка отчета о проделанной работе.
Тема 2.2 Симметричные криптосистемы	*Лекция (2 час.)*	Связь ключа и алгоритма. Методы шифрования. Преимущества и недостатки симметричных и ассиметричных криптостистем. Блочные и потоковые шифры: принципы построения. Сеансовый ключ. Гибридные методы шифрования. Технология цифрового конверта. -принцип работы современных симметричных криптостистем на примере алгоритма шифрования ГОСТ 28147-89
	Практическое занятие (2 час.)	**Практическое задание № 3**. Изучение алгоритма шифрования ГОСТ 28147-89. Изучить работу алгоритма шифрования ГОСТ 28147-89. Осуществить один цикл шифрования текста с применением ГОСТ 28147-89 в режиме простой замены.
	Самостоятельная работа (2 час.)	**Практическое задание № 3**Осуществить один цикл шифрования текста с применением ГОСТ 28147-89 в режиме простой замены. Подготовка и отправка отчета о проделанной работе.
Тема 2.3 Криптосистемы с открытым ключом	*Лекция (2 час)*	Алгоритмы Диффи-Хеллмана, RSA, ELGAMAL, Меркля-Хеллмана и Эль-Гамаля Эллиптическая криптография. Алгоритмы, основанные на «последовательностях Люка». Ранцевая криптосистема: принцип работы. Протокол доказательства с нулевым разглашением.
	Практическое занятие (2 час.)	**Практическое задание № 4.** Криптографические алгоритмы с открытым ключом. Изучить алгоритмы шифрования RSA, Меркля-Хеллмана, Эль-Гамаля. Зашифровать и расшифровать заданное сообщение с помощью указанных алгоритмов.
	Самостоятельная работа (2 час.)	**Практическое задание № 4.** Зашифровать и расшифровать заданное сообщение с помощью алгоритмов шифрования RSA, Меркля-Хеллмана, Эль-Гамаля Подготовка и отправка отчета о проделанной работе.
Тема 2.4 Хэш-функции в криптографии	*Лекция (2 час.)*	Определение хэш-функций. Их виды. Способы построения. Безопасное хэширование схемы. Коллизии хэш-функций и их виды. Методы поиска коллизий. Обзор современных алгоритмов хэширования.

	Практическое занятие (2 час.)	**Практическое задание № 5**. Хэш-функция MD5. Изучить алгоритм хэширования MD5. Вычислить по этому алгоритму хэш от заданного сообщения.
	Самостоятельная работа (2 час.)	**Практическое задание № 5** Вычислить по э алгоритму хэширования MD5 хэш от заданного сообщения Подготовка и отправка отчета о проделанной работе.
Тема 2.5 Цифровая подпись	*Лекция (2 час.)*	Понятие аутентификации данных и цифровая подпись. Проблема аутентификации данных и электронная цифровая подпись. История возникновения ЭЦП. Основные понятия и определения. Алгоритмы ЭЦП. Подделка подписей. Меры по защите от подделки цифровых подписей. Способы управление ключами цифровых подписей. Алгоритмы формирования и проверки цифровой подписи к заданному сообщению по алгоритмам RSA, ELGAMAL и DSA.
	Практическое занятие (2 час.)	**Практическое задание № 6.** Формирование и проверка ЭЦП. Изучить алгоритмы цифровой подписи RSA, ELGAMAL и DSA. Сформировать и проверить подписи к заданному сообщению по указанным алгоритмам.
	Самостоятельная работа (2 час.)	**Практическое задание № 6.** Сформировать и проверить подписи к заданному сообщению по алгоритмам цифровой подписи RSA, ELGAMAL и DSA Подготовка и отправка отчета о проделанной работе.
Тема 2.6 Стеганография	*Лекция (2 час.)*	Определение и основные понятия стеганографии. История развития стеганографии как науки. Основные требования к стегосистемам. Виды контейнеров с стегосистемам и требования к ним. Применение стеганографии в кибербезопасности. Алгоритмы встраивания информации в мультимедийные файлы и в программное обеспечение.
	Практическое занятие (2 час.)	**Практическое задание № 7.** Защита программного обеспечения методами стеганографии. Изучить методы защиты исполняемых файлов. Произвести встраивание заданной информации в программный файл и ее последующее извлечение.
	Самостоятельная работа (2 час.)	**Практическое задание № 7.** Произвести встраивание заданной информации в программный файл и ее последующее извлечение. Подготовка и отправка отчета о проделанной работе.
Раздел 3. Противодействие вредоносному программному обеспечению.		
Тема 3.1 Вредоносное программное обеспечение	*Лекция (4 час.)*	Вирусы. Общее определение. Файловые, загрузочные, файлово-загрузочные вирусы. Стелс-вирусы. Шифрующиеся, полиморфные, макрокомандные вирусы. Вирусы в пакетных

		файлах ОС и в драйверах. Известные и неизвестные вирусы. Типичные симптомы вирусной атаки. Черви: определение, свойства и способы противодействия распространению. Логические бомбы и их особенности. Троянские объекты: определение, свойства и способы противодействия распространению. Программы backdoor и их особенности. Шпионское программное обеспечение: разновидности, опасности. Программы adware: разновидности, опасности. Алгоритм определения типа заданных описанием программ по классификации лаборатории Касперского.
	Практическое занятие (2 час.)	**Решение кейсов № 2.** Детектирование вредоносных программ. Изучить классификацию вредоносного программного обеспечения, принятую в лаборатории Касперского. Определить тип заданных описанием программ по этой классификации.
	Самостоятельная работа (2 час.)	**Решение кейсов № 2.** Определить тип заданных описанием программ по классификации лаборатории Касперского. Подготовка и отправка отчета о проделанной работе.
Тема 3.2 Системы антивирусной защиты	*Лекция (2 час.)*	Принципы построения систем антивирусной защиты. Требования к антивирусным пакетам. Состав антивирусного пакета. Основные методы антивирусной защиты. Алгоритм проверки работы антивирусных программ с помощью тестовых вирусов.
	Практическое занятие (2 час.)	**Практическое задание № 8.** Тестирование работы антивируса. Изучить методику применения тестовых вирусов для проверки работы антивирусных программ. Выполнить тестирование работы антивируса с помощью алгоритма проверки работы антивирусных программ с помощью тестовых вирусов.
	Самостоятельная работа (2 час.)	**Практическое задание № 8.** Выполнить тестирование работы антивируса на основании алгоритма проверки работы антивирусных программ с помощью тестовых вирусов. Подготовка и отправка отчета о проделанной работе.
Тема 3.3 Сетевая безопасность	*Лекция (2 час.)*	Определение сетевого экрана. Основные задачи и режимы работы сетевого экрана. Критерии качества работы сетевого экрана. Утечки. Базовые идеи и технологии, позволяющие обойти защиту сетевого экрана. Виды наиболее распространенных сетевых атак. Алгоритм разработки учебного занятия о сетевых атаках и способах противодействия им.

	Практическое занятие (3 час.)	**Проект № 1.** Сетевые атаки. Изучить классификацию сетевых атак и основные меры противодействия им. Разработать учебное занятие с презентацией о конкретной сетевой атаке (угрозе) и способах противодействия ей.
	Самостоятельная работа (6 час.)	**Проект № 1.** Разработать учебное занятие с презентацией о конкретной сетевой атаке (угрозе) (по выбору обучающегося) и способах противодействия ей. Подготовка и отправка отчета о проделанной работе.
Итоговая аттестация	*Итоговое тестирование (1 час)*	Зачет на основании совокупности выполненных работ + результаты итогового тестирования

3. Форма аттестации и оценочные материалы

Итоговая аттестация осуществляется на основании совокупности работ, выполненных на положительную оценку, а также по результатам защиты проекта и итогового тестирования.

В ходе обучения планируется создать образовательный продукт, применимый в практике преподавания дисциплины «Информатика и информационно-коммуникационные технологии» в старших классах средней школы – проект, включающий в себя разработку учебного занятия с презентацией о конкретной сетевой атаке (угрозе) и способах противодействия ей и презентацию, выполненную в программе MS Power Point.

Приведенные ниже оценочные материалы позволяют диагностировать достижение планируемых результатов обучения.

3.1 Форма текущей аттестации

Текущая аттестация включает в себя оценки за отчеты по практическим работам и оценки за решение кейсов.

3.1.1. Требования к оформлению отчетов по практическим работам.

Отчет по практическим работам оформляется в электронном виде и пересылается преподавателю через электронную образовательную среду CANVAS или по электронной почте.

Отчет должен содержать постановку задачи, необходимые формулы и результаты расчетов. В конце отчета должен быть сделан вывод о проделанной работе и ответы на контрольные вопросы по варианту задания

3.1.2. Критерии оценивания практических работ и кейсов.

Каждая практическая работа оценивается по пятибалльной шкале. Критерии оценивания приведены в таблице.

Критерий	Детализация критерия			Баллы (макс.)
Выполнение расчетов	расчеты выполнены неверно (0 баллов)	есть незначительные ошибки (1 балл)	расчеты выполнены верно (2 балла)	2
Ответ на контрольные вопросы	нет ответов или ответы неверные (0 баллов)		верные ответы (1 балл)	1
Полнота оформления	работа оформлена с нарушением (нет постановки задачи, формул, выводов) или небрежное оформление (0 баллов)		работа содержит все необходимые части (1 балл)	1
Своевременность сдачи работы	работа сдана с опозданием (0 баллов)		работа сдана вовремя (1 балл)	1
			Итого	5

Участие в решении кейсов оценивается в 5 баллов. В случае отсутствия обучающегося за решение кейса выставляется 0 баллов.

3.1.3. Примеры тем практических заданий

Задание 1. Количественная оценка стойкости парольной защиты.

1. Заданы следующие параметры парольной системы: скорость перебора паролей $V = 1 \cdot 10^5$ паролей в секунду, вероятности подбора пароля P в течение срока его действия: $P_1 = 10^{-11}$, $P_2 = 10^{-9}$, $P_3 = 10^{-7}$, $P_4 = 10^{-5}$, $P_5 = 10^{-3}$ и сроки действия пароля T: $T_1 = 30$ суток, $T_2 = 45$ суток, $T_3 = 60$ суток, $T_4 = 90$ суток.

Рассчитать соответствующие длины пароля при A, равных 36 (сумма букв латинского алфавита одного регистра и цифр) и 62 (сумма букв латинского алфавита верхнего и нижнего регистров и цифр) символам.

Построить графики изменения длин паролей в зависимости от значения вероятностей подбора пароля в течение фиксированных сроков жизни пароля при алфавите, равном 36 и 62 символам.

Согласно полученным результатам и построенным графику сделать выводы о длине и структуре пароля при заданной вероятности его перебора.

2. Заданы следующие параметры парольной системы: скорость перебора паролей $V = 1 \cdot 10^4$ паролей в секунду, вероятности подбора пароля P в течение срока его действия: $P_1 = 10^{-11}$, $P_2 = 10^{-9}$, $P_3 = 10^{-7}$, $P_4 = 10^{-5}$, $P_5 = 10^{-3}$ и длины паролей L: $L_1 = 8$, $L_2 = 9$, $L_3 = 10$.

Рассчитать соответствующие вероятности подбора пароля при A, равных 36 и 62 символам. Построить графики изменения вероятностей подбора пароля в зависимости от изменения длин паролей в течение фиксированных сроков жизни пароля и алфавитах, равном 36 и 62 символам.

По результатам проведенных расчетов сделать вывод о путях уменьшения вероятности подбора пароля.

Задание 2. Криптографическая защита информации

1. Зашифровать свои фамилию, имя, отчество шифром Виженера. В качестве ключа использовать случайную последовательность из 5 символов. Проверить правильность шифрования путем расшифрования на том же ключе.

2. Зашифровать свою фамилию с помощью следующих шифров:

- алгоритма RSA;
- алгоритма на основе задачи об укладке ранца;
- алгоритма шифрования Эль-Гамаля.

При оформлении отчета необходимо привести исходное сообщение (фамилию) и таблицы генерации ключей, шифрования и расшифрования. Для первого и третьего способов принять, что код символа соответствует его положению в алфавите, для второго – в соответствии с кодировкой Windows 1251. Для нахождения первообразного корня допускается использование таблицы первообразных корней простых чисел до 1000.

3. Найти хеш–образ первых шести букв своей фамилии, используя хеш-функцию $H_i = (H_{i-1}+M_i)^2 \bmod n$, где $n = pq$, p, q – простые числа в пределах 100. Принять, что буквам соответствуют их порядковые номера в алфавите.

4. Используя хеш-образ, полученный в п. 3 и закрытый ключ, полученный в п.2, вычислить электронную цифровую подпись по схеме RSA.

5. Проверить правильность ЭЦП, полученной в п. 4, используя открытый ключ, полученный в п.2 и значение хэш-функции, полученное в п.3.

6. Используя хеш-образ, полученный в п. 3, вычислить электронную цифровую подпись по схеме Эль-Гамаля.

7. Проверить правильность ЭЦП, полученной в п. 6, используя значение хэш-функции, полученное в п.3.

8. Используя хеш-образ, полученный в п. 3, вычислить электронную цифровую подпись по схеме DSA.

9. Проверить правильность ЭЦП, полученной в п. 8, используя значение хэш-функции, полученное в п.3.

3.1.4. Примеры вопросов к защите практических работ

1. Как происходит процесс генерации ключей в алгоритме цифровой подписи RSA?

2. Что произойдет, если поменять местами открытый и закрытый ключи в алгоритме цифровой подписи RSA?

3. Какие требования предъявляются к криптографическим хеш-функциям?

4. Дайте определение коллизии хэш-функции. Приведите примеры.

5. Чем отличается коллизия первого рода от коллизии второго рода?

6. В чём заключаются процессы генерации ключа и постановки подписи в алгоритме Эль-Гамаля?

7. Как проверяется правильность цифровой подписи в алгоритме DSA?

8. Какие требования предъявляются к средствам постановки электронной подписи?

9. Каким образом можно находить коллизии хеш-функций?

3.2 Форма итоговой аттестации

Форма итоговой аттестации – зачет как совокупность выполненных на положительную оценку практических работ, теста и проекта. Итоговая аттестация осуществляется на основании полученных совокупных баллов за практические работы, тест и проект.

Оценивание: зачет/незачет. Зачет выставляется в случае, если обучающимся набрано за практические работы, тест и проект в сумме не менее 45 баллов.

3.2.1. Описание итогового теста и его шкалы оценивания.

Итоговый тест состоит из 10 вопросов по всем разделам курса. Правильный ответ на каждый вопрос оценивается в 1 балл. Тест считается пройденным и засчитывается в случае не менее 7 правильных ответов.

3.2.2. Описание проекта и его шкалы оценивания.

Проект представляет собой план-конспект урока по разделу «Кибербезопасность» и состоит из краткой пояснительной записки (не более 10 страниц) и презентации, выполненной в программе MS Power Point. В основе проекта лежит описание и анализ конкретной сетевой атаки или уязвимости, выбираемой по указанию преподавателя.

Для оформления текста пояснительной записки рекомендуется придерживаться требований ГОСТ 7.32-2001 «Отчет о научно-исследовательской работе».

Пояснительная записка оформляется на листах бумаги стандартного формата А4 (210х297). Текст размещается на одной стороне листа.

Размеры полей: левое – 2 см, правое – 1 см, верхнее – 2 см, нижнее – 2 см.

Используется полуторный межстрочный интервал. Для основного текста используется шрифт Times New Roman, размер (кегль) 14 пунктов. Для заголовков рекомендуется использовать шрифт Arial.

Абзацный отступ составляет 1.25 см. Абзацы выравниваются по ширине. До и после абзаца – нулевой интервал (т.е. абзацы не отделяются друг от друга дополнительными «пустыми строчками»).

Все страницы имеют сквозную нумерацию, начиная с титульного листа. На титульном листе номер не проставляется. Номер страницы в нижнем поле, по центру.

Оценка проекта проводится по пятибалльной системе. Шкала критериев приведена в таблице.

Критерий	Детализация критерия		Баллы (макс.)
Самостоятельность выполнения проекта	Работа выполнена не самостоятельно, с большим количеством заимствований (0 баллов)	Работа выполнена самостоятельно (0 баллов)	1
Практическая значимость	Работа не имеет практической значимости (0 баллов)	Работа имеет практическую значимость и может быть использована в учебном процессе (1 балл)	1
Структура и оформление	Работа оформлена с нарушением требований или небрежное оформление (0 баллов)	Работа оформлена правильно (1 балл)	1
Презентация проекта	Не использованы никакие наглядно-иллюстративные средства, плохо выстроена логика выступления, нет ответов на дополнительные вопросы (0 баллов)	Выстроена логика выступления, оптимально использованы наглядно-иллюстративные средства раскрывающие тему, четко и лаконично даны ответы на все заданные вопросы, соблюден регламент, речь соответствует правилам публичного выступления (1 балл)	1
Своевременность сдачи работы	работа сдана с опозданием (0 баллов)	работа сдана вовремя (1 балл)	1
		Итого	5

3.2.3. Пример итогового теста

1. Существенными признаками понятия «информационная безопасность» являются:
   а) конфиденциальность;
   б) секретность;
   в) устойчивость к взлому;
   г) целостность;
   д) надёжность;
   е) доступность.
2. Сведения о лицах, предметах, фактах, событиях, явлениях и процессах независимо от формы их представления – это:

а) документированная информация;

б) информация;

в) конфиденциальная информация;

г) документ.

3. По конечному проявлению различают следующие угрозы информации (выберите несколько ответов):

а) блокирование;

б) ознакомление;

в) структурирование;

г) взлом;

д) модификация;

е) уничтожение.

1. Какой алгоритм применяется для реализации протокола идентификации с нулевым разглашением:
   a) алгоритм Диффи-Хеллмана;
   b) алгоритм Эль-Гамаля;
   c) алгоритм Меркля;
   d) алгоритм Фейга-Фиата-Шамира.
2. Какой алгоритм не является алгоритмом с открытым ключом:
   a) алгоритм RSA;
   b) алгоритм Эль-Гамаля;
   c) алгоритм DES;
   d) алгоритм LUC.
3. Какой алгоритм не является алгоритмом криптографического хэширования:
   a) алгоритм MD5;
   b) алгоритм CRC 32;
   c) алгоритм SHA;
   d) алгоритм ГОСТ 34.11-94.
4. Какой вирус пользуется для шифрования специальными паролями (ключами), а также различными методами шифрования, что исключает его опознавание по сигнатурам:
   a) файлово-загрузочный вирус;
   b) полиморфный вирус;
   c) стелс-вирус;
   d) макрокомандный вирус.
5. Какие вирусы заражают носители данных:
   a) файловые;
   b) загрузочные;

c) макровирусы;
d) сетевые черви.

6. К недостаткам эвристических методов антивирусного анализа относятся:
   a) ложные срабатывания;
   b) невозможность лечения вируса;
   c) необходимость постоянного обновления антивирусных баз;
   d) невысокая эффективность.
7. Ниже перечислено несколько файлов. Укажите системный компонент Windows, который нужно разрешить в сетевом экране для работы с интернетом.
   a) notepad.exe;
   b) svchost.exe;
   c) regedit32.exe;
   d) winmine.exe.

Раздел 4 Организационно-педагогические условия реализации программы

4.1 Учебно-методическое обеспечение и информационное обеспечение программы

4.1.1 Основная литература

1 Бабенко Л. К. Криптографическая защита информации: симметричное шифрование : учебное пособие для вузов / Л. К. Бабенко, Е. А. Ищукова. — М. : Юрайт, 2019. — 220 с.

2 Нестеров С. А. Информационная безопасность : учебник и практикум для академического бакалавриата / С. А. Нестеров. — М. : Юрайт, 2019. — 321 с.

4.1.2 Дополнительная литература

3 Баранова Е.К., Бабаш А.В. Информационная безопасность и защита информации. – М.: ИНФРА-М РИОР, 2016. – 322 с.

4 Бахаров Л.Е. Информационная безопасность и защита информации. Методические указания к практическим занятиям и самостоятельной работе студентов по направлению 230200 - «Информационные системы» по специальности 230201 - «Информационные системы и технологии». – М.: МГГУ, 2012. – 63 с.

5 Бахаров Л.Е. Информационная безопасность и защита информации. Методические указания по выполнению контрольных заданий и самостоятельной работе студентов по направлению 230200 - «Информационные системы» по специальности 230201 - «Информационные системы и технологии». – М.: МГГУ, 2011. – 31 с.

6 Бахаров Л.Е. Информационная безопасность и защита информации. Сборник тестов. – М.: Издательский дом МИСИС, 2015. – 42 с.

7 Васильева И. Н. Криптографические методы защиты информации : учебник и практикум для академического бакалавриата / И. Н. Васильева. — М. : Юрайт, 2019. — 349 с.
8 Запечников С. В. Криптографические методы защиты информации : учебник для академического бакалавриата / С. В. Запечников, О. В. Казарин, А. А. Тарасов. — М. : Юрайт, 2019. — 309 с.
9 Лось А. Б. Криптографические методы защиты информации для изучающих компьютерную безопасность : учебник для академического бакалавриата / А. Б. Лось, А. Ю. Нестеренко, М. И. Рожков. — 2-е изд., испр. — М. : Юрайт, 2019. — 473 с.
10 Фомичёв В. М. Криптографические методы защиты информации в 2 ч. Часть 1. Математические аспекты : учебник для академического бакалавриата / В. М. Фомичёв, Д. А. Мельников ; под редакцией В. М. Фомичёва. — М. : Юрайт, 2019. — 209 с.
11 Фомичёв, В. М. Криптографические методы защиты информации в 2 ч. Часть 2. Системные и прикладные аспекты : учебник для академического бакалавриата / В. М. Фомичёв, Д. А. Мельников ; под редакцией В. М. Фомичёва. — Москва : Издательство Юрайт, 2019. — 245 с.

4.2 Материально-технические условия реализации программы

1) Специализированные лаборатории и классы, основные установки и стенды.
2) Компьютерные программы: MathCad, MATLAB, Electronics Workbench (MultiSim);
3) Доступ в локальную сеть и ИНТЕРНЕТ для использования электронных ресурсов;
4) Пакет MS Office или аналогичный для оформления отчетов по выполненным работам.

4.3. Интернет-ресурсы

1 http://www.fstec.ru/ Сайт Федеральной службы по техническому и экспортному контролю, содержит перечень правовых, организационно-распорядительных, нормативных документов по технической защите информации, принятых в Российской Федерации (дата обращения: 19.10.2019);
2 https://bdu.fstec.ru/ Банк данных угроз безопасности информации (дата обращения: 19.10.2019);
3 http://citforum.ru/security/ Статьи, обзоры, книги по информационной безопасности (дата обращения: 19.10.2019);
4 http://www.itsec.ru/main.php Сайт журнала «Информационная безопасность» (дата обращения: 19.10.2019);

5 http://www.securelist.com/ru/threats Вирусная энциклопедия "Лаборатории Касперского", содержит хорошо структурированные и оперативно обновляемые описания электронных угроз и способы их предотвращения (дата обращения: 19.10.2019);

6 http://www.npo-echelon.ru/about/articles.php Материалы по информационной безопасности на сайте НПО "Эшелон" (дата обращения: 19.10.2019).