МИНИСТЕРСТВО НАУКИ И ВЫСШЕГО ОБРАЗОВАНИЯ РОССИЙСКОЙ ФЕДЕРАЦИИ

ФЕДЕРАЛЬНОЕ ГОСУДАРСТВЕННОЕ БЮДЖЕТНОЕ ОБРАЗОВАТЕЛЬНОЕ УЧРЕЖДЕНИЕ ВЫСШЕГО ОБРАЗОВАНИЯ

«ВОРОНЕЖСКИЙ ГОСУДАРСТВЕННЫЙ УНИВЕРСИТЕТ ИНЖЕНЕРНЫХ ТЕХНОЛОГИЙ»

ДОКУМЕНТ ПОДПИСАН ЭЛЕКТРОННОЙ ПОДПИСЬЮ

Сертификат: 00A29CA99D98126F4EB57F6F989D713C88
Владелец: Василенко Виталий Николаевич
Действителен: с 07.07.2022 до 30.09.2023

УТВЕРЖДАЮ

Проректор по учебной работе

_____ ___Василенко В.Н.___
(подпись) (Ф.И.О.)

«25» мая 2023 г.

РАБОЧАЯ ПРОГРАММА ДИСЦИПЛИНЫ

Методы и средства криптографической защиты информации
(наименование в соответствии с РУП)

Направление подготовки (специальность)

10.05.03 Информационная безопасность автоматизированных систем
(шифр и наименование направления подготовки/специальности)

Направленность (профиль)

Безопасность открытых информационных систем
(наименование профиля/специализации)

Квалификация выпускника
Квалификация: специалист по защите информации

Воронеж

1. Цели и задачи дисциплины

Целью освоения дисциплины (модуля) является формирование компетенций обучающегося в области профессиональной деятельности и сфере профессиональной деятельности:
Разработка систем защиты информации автоматизированных систем, формирование требований к защите информации в автоматизированных системах. Дисциплина направлена на решение задач профессиональной деятельности
-научно исследовательского типа: обоснование необходимости защиты информации в автоматизированной системе, моделирование защищенных автоматизированных систем с целью анализа их уязвимостей и эффективности средств и способов защиты информации
- проектного типа: разработка проектных решений по защите информации в автоматизированных системах

Программа составлена в соответствии с требованиями Федерального государственного образовательного стандарта высшего образования по направлению специальности 10.05.03 Информационная безопасность автоматизированных систем.

2. Перечень планируемых результатов обучения, соотнесенных с планируемыми результатами освоения образовательной программы

№ п/п	Код компетенции	Формулировка компетенции	Код и наименование индикатора достижения компетенции
1	*ОПК-10*	*Способен использовать средства криптографической защиты информации при решении задач профессиональной деятельности;*	*ИД2опк-10 – владеет методами и средствами криптографической защиты информации при решении задач профессиональной деятельности*

Код и наименование индикатора достижения компетенции	Результаты обучения (показатели оценивания)
ИД2опк-10 – владеет методами и средствами криптографической защиты информации при решении задач профессиональной деятельности	Знает: основные классы шифров, способы их реализации; программно-аппаратные средства реализации криптографических систем защиты информации; типовые поточные и блочные шифры, а также асимметричные криптосистемы; основные крипто-графические протоколы системы шифрования с открытыми ключами
	Умеет: применять методы описания и исследования криптосистем; кодировать алгоритмы с соблюдением требований к качественному стилю программирования; определять структуру оптимальных устройств обработки сигналов информационных радиотехнических систем
	Владеет: навыками использования основных типов шифров и криптографических алгоритмов при решении задач обеспечения информационной безопасности; методами оценки криптографической стойкости алгоритмов шифрования; криптографической терминологией

3. Место дисциплины в структуре ОП ВО

Дисциплина относится к обязательной части Блока 1 ООП. Дисциплина является обязательной к изучению.

Изучение дисциплины основано на знаниях, умениях и навыках, полученных при изучении обучающимися дисциплин «Основы информационной безопасности», «Безопасность персональных данных», «Информационная безопасность открытых систем».

Дисциплина является предшествующей для изучения последующих дисциплин «Защита информации от утечки по техническим каналам», «Средства проектирования для аппаратных средств защиты информации». Знания, полученные входе изучения дисциплины, используются при подготовке к ГИА.

4. Объем дисциплины и виды учебных занятий

Общая трудоемкость дисциплины составляет 7 зачетных единиц.

Виды учебной работы	Всего академических часов	7 семестр	8 семестр
		Акад. ч	Акад. ч
Общая трудоемкость дисциплины (модуля)	**252**	**108**	**144**
Контактная работа в т. ч. аудиторные занятия:	**118,7**	**55**	**63,7**
Лекции	48	30	18
в том числе в форме практической подготовки	–	–	–
Практические занятия	66	30	36
в том числе в форме практической подготовки	–	–	–
Текущие консультации	6,6	1,5	4,6
Вид аттестации – зачет	0,1	0,1	
Вид аттестации – экзамен	33,8		33,8
Самостоятельная работа:	**98**	**46,4**	**51,6**
Подготовка доклада с презентацией	15	7,5	7,5
Подготовка к коллоквиуму	22,5	11,25	11,25
Домашнее задание	46,4	27,65	18,75
Курсовая работа	14,1		14,1

5. Содержание дисциплины, структурированное по темам (разделам) с указанием от-веденного на них количества академических часов и видов учебных занятий

5.1 Содержание разделов дисциплины

№ п/п	Наименование разделов дисциплины	Содержание раздела	
1	Организация криптографической передачи информации	Характер криптографической деятельности; простейшие шифры и их свойства; композиции шифров; системы шифрования с открытыми ключами; виды информации, подлежащие закрытию, их модели и свойства; криптографическая стойкость шифров. Требования к защи- те информации, оценка возможностей противоборствующей сторо- ны. Методология разработки и анализа средств защиты. Классиче- ские модели защиты информации. Стеганографические и криптогра- фические методы защиты информации. Математические модели криптосистемы. Симметричные и асимметричные криптосистемы. Вопросы распределения ключей в сети шифрованной связи.	
2	Криптографические системы и их характеристики	Определение шифра. Модели шифров. Ключевая система шифра. Основные требования к шифрам. Простейшие шифры и их свойства. Композиции шифров. Синтез шифров. Классификация шифров. Шифры замены. Шифры перестановки. Табличное и модульное гам- мирование. Случайные и псевдослучайные гаммы. Совершенные шифры; теоретикоинформационный подход к оценке криптостойко- сти шифров; вопросы практической стойкости; имитостойкость и помехоустойчивость шифров	

3	Реализация криптографических протоколов и ал-	Концепция криптосистемы с открытым ключом. Однонаправленные (односторонние) функции. Криптосистемы RSA. Криптосистемы	
	горитмов	Эль-Гамаля. Теоретико-информационный подход к оценке крипто- стойкости шифров. Избыточность языка. Совершенные шифры и расстояние единственности. Принципы построения криптографиче- ских алгоритмов; различие между программными и аппаратными реализациями; криптографические параметры узлов и блоков шифраторов; синтез шифров	
4	Блочные шифры. Поточное шифрование	Методы криптоанализа поточных шифров. Особенности криптоана- лиза блочных шифров. Имитация и подмена сообщения. Характери- стики и методы обеспечения имитостойкости. Совершенная имито- стойкость. Основные способы реализации криптографических алго- ритмов и требования, предъявляемые к ним. Принципы построения блочных шифров. Поточные системы шифрования. Методы получения случайных и псевдослучайных последовательностей; программ- ные реализации шифров	
5	Концептуальный подход к защите информации в компьютерных системах и сетях	Регистры сдвига с обратной связью. Линейные рекуррентные после- довательности. Свойства псевдослучайных последовательностей. Основные элементы средств защиты сети от несанкционированного доступа. Особенности использования вычислительной техники в криптографии; вопросы организации сетей засекреченной связи; ключевые системы; криптографические хеш-функции; электронная цифровая подпись	

5.2 Разделы дисциплины и виды занятий

№ п/п	Наименование раздела дисциплины	Лекции, час	ЛР, час	ПЗ, час	СР, час
1	Организация криптографической передачи информации	8	-	12	23,2
2	Криптографические системы и их характеристики	8	-	12	23,2
3	Реализация криптографических протоколов и алгоритмов	8	-	12	18,75
4	Блочные шифры. Поточное шифрование	8	-	12	10
5	Концептуальный подход к защите информации в компьютерных системах и сетях	16	-	18	14,11
	ИТОГО	48	-	66	8,75

5.2.1 Лекции

№ п/п	Наименование раздела дисциплины	Тематика лекционных занятий	Трудоемкость, Час

1	Организация криптографической передачи информации	Характер криптографической деятельности; простейшие шифры и их свойства; композиции шифров; системы шифрования с открытыми ключами; виды информации, подлежащие закрытию, их модели и свойства; криптографическая стойкость шифров. Требования к защите информации, оценка возможностей противоборствующей стороны. Методология разработки и анализа средств защиты. Классические модели защиты информации. Стеганографические и криптографические методы защиты информации. Математические модели криптосистемы. Симметричные и асимметричные криптосистемы. Вопросы распределения ключей в сети шифрованной связи.	8
2	Криптографические системы и их характеристики	Определение шифра. Модели шифров. Ключевая система шифра. Основные требования к шифрам. Простейшие шифры и их свойства. Композиции шифров. Синтез шифров. Классификация шифров. Шифры замены. Шифры перестановки. Табличное и модульное гаммирование. Случайные и псевдослучайные гаммы. Совершенные шифры; теоретикоинформационный подход к оценке криптостойкости шифров; вопросы практической стойкости; имитостойкость и помехоустойчивость шифров	8
3	Реализация криптографических протоколов и алгоритмов	Концепция криптосистемы с открытым ключом. Однонаправленные (односторонние) функции. Криптосистемы RSA. Криптосистемы Эль-Гамаля. Теоретико-информационный подход к оценке криптостойкости шифров. Избыточность языка. Совершенные шифры и расстояние единственности. Принципы построения криптографических алгоритмов; различие между программными и аппаратными реализациями; криптографические параметры узлов и блоков шифраторов; синтез шифров	8
4	Блочные шифры. Поточное шифрование	Методы криптоанализа поточных шифров. Особенности криптоанализа блочных шифров. Имитация и подмена сообщения. Характеристики и методы обеспечения имитостойкости. Совершенная имитостойкость. Основные способы реализации криптографических алгоритмов и требования, предъявляемые к ним. Принципы построения блочных шифров. Поточные системы шифрования. Методы получения случайных и псевдослучайных последовательностей; программные реализации шифров	8
5	Концептуальный подход к защите информации в компьютерных системах и сетях	Регистры сдвига с обратной связью. Линейные рекуррентные последовательности. Свойства псевдослучайных последовательностей. Основные элементы средств защиты сети от несанкционированного доступа. Особенности использования вычислительной техники в криптографии; вопросы организации сетей засекреченной связи; ключевые системы; криптографические хеш-функции; электронная цифровая подпись	16
	Итого		48

5.2.2 Практические занятия

№ п/п	Наименование раздела дисциплины	Тематика практических занятий	Трудоемкость, час
1	Организация криптографической передачи информации	Открытые сообщения, организация шифровальной связи. Синтез шифров замены и гаммирования. Синтез систем шифрования с открытыми ключами	12
2	Криптографические системы и их характеристики	Методы анализа криптографических алгоритмов. Имитостойкость и помехоустойчивость шифров. Протоколы сертификации и распределения ключей. Протоколы выработки сеансовых ключей. Протоколы выработки сеансовых ключей.	12
3	Реализация криптографических протоколов и алгоритмов	Синтез систем шифрования с открытыми ключами. Совершенные шифры. Безусловно стойкие и вычислительно стойкие шифры. Помехоустойчивость шифров. Помехоустойчивое кодирование	12
4	Блочные шифры. Поточное шифрование	Программные реализации шифров. Исследование криптографических свойств шифров замены и гаммирования. Исследование криптографических свойств шифрсистем поточного типа.	12
5	Концептуальный подход к защите информации в компьютерных системах и сетях	Исследование криптографических свойств шифрсистем с открытым ключом. Открытое распределение ключей Диффи-Хеллмана и его модификации. Система распределения ключей ЭЦП. Инфраструктура открытых ключей. Программные комплексы Crypton Word и Crypton Excel.	18
	Итого		66

5.2.3 Лабораторный практикум не предусмотрен

5.2.4 Самостоятельная работа обучающихся (СРО)

№ п/п	Наименование раздела дисциплины	Вид СРО	Трудоемкость, час
1	Организация криптографической передачи информации	Подготовка к коллоквиуму	23,2
2	Криптографические системы и их характеристики	Домашнее задание «Открытые сообщения, организация шифровальной связи»	23,2
3	Реализация криптографических протоколов и алгоритмов	Подготовка к коллоквиуму	18,75
4	Блочные шифры. Поточное шифрование	Подготовка доклада	10
5	Концептуальный подход к защите информации в компьютерных системах и сетях	Курсовая работа	14,1
	Итого		8,75

6 Учебно-методическое и информационное обеспечение дисциплины

6.1 Основная литература

1. Каширская, Е. Н. Основы криптографического анализа : учебное пособие / Е. Н. Каширская. — Москва : РТУ МИРЭА, 2020. — 74 с. — Текст : электронный // Лань : электронно-библиотечная система. — URL: https://e.lanbook.com/book/163805

2. Каширская, Е. Н. Криптографический анализ и методы защиты информации : учебное пособие / Е. Н. Каширская. — Москва : РТУ МИРЭА, 2020. — 91 с. — Текст : электронный // Лань : электронно-библиотечная система. — URL: https://e.lanbook.com/book/163861

3. Ермакова, А. Ю. Криптографические методы защиты информации : учебно-методическое пособие / А. Ю. Ермакова. — Москва : РТУ МИРЭА, 2021. — 172 с. — Текст : электронный // Лань : электронно-библиотечная система. — URL: https://e.lanbook.com/book/176563

6.2. Дополнительная литература

1. Данилов, А. Н. Математические основы криптологии и криптографические методы и средства обеспечения информационной безопасности : учебное пособие / А. Н. Данилов, Е. Л. Кротова, Ю. Н. Липин. — Пермь : ПНИПУ, 2008. — 364 с. — ISBN 978-5-398-00076-4. — Текст : электронный // Лань : электронно-библиотечная система. — URL: https://e.lanbook.com/book/160834

2. Прохорова, О. В. Информационная безопасность и защита информации : учебник / О. В. Прохорова. — 2-е изд., испр. — Санкт-Петербург : Лань, 2020. — 124 с. — ISBN 978-5-8114-4404-5. — Текст : электронный // Лань : электронно-библиотечная система. — URL: https://e.lanbook.com/book/133924

3. Корниенко, А. А. Криптографические методы защиты информации : учебное пособие / А. А. Корниенко, М. Л. Глухарев. — Санкт-Петербург : ПГУПС, 2018 — Часть 2 — 2018. — 63 с. — ISBN 978-5-7641-1215-2. — Текст : электронный // Лань : электронно-библиотечная система. — URL: https://e.lanbook.com/book/138103

6.3 Перечень учебно-методического обеспечения для самостоятельной работы обучающихся

Криптографические методы защиты информации: методические указания для самостоятельной работы для студентов, обучающихся по направлению 10.05.03– «Информационная безопасность автоматизированных систем», очной формы обучения / А. В. Скрыпников**,** Е. В. Чернышова ; ВГУИТ, Кафедра информационной безопасности. - Воронеж : ВГУИТ, 2021. - 11 с.

6.3 Перечень ресурсов информационно-телекоммуникационной сети «Интернет», необходимых для освоения дисциплины

1. Сайт научной библиотеки ВГУИТ <http://cnit.vsuet.ru>.

2. Электронно-библиотечная система ЛАНЬ <https://e.lanbook.com>.

3.ЭБС «Университетская библиотека Онлайн» <https://biblioclub.ru/>.

4. Базовые федеральные образовательные порталы. <http://www.edu.ru/db/portal/sites/portal_page.htm>.

5. Государственная публичная научно-техническая библиотека. <www.gpntb.ru/>.

6. Информационно-коммуникационные технологии в образовании. Система феде- ральных образовательных порталов. <http://www.ict.edu.ru/>.

7. Национальная электронная библиотека. <www.nns.ru/>..

8. Поисковая система «Апорт». <www.aport.ru/>.

9. Поисковая система «Рамблер». <www.rambler.ru/>.

10. Поисковая система «Yahoo» . <www.yahoo.com/>.

11. Поисковая система «Яндекс». <www.yandex.ru/>.

12. Российская государственная библиотека. <www.rsl.ru/>.

6.5 Перечень информационных технологий, используемых при осуществлении образовательного процесса по дисциплине (модулю), включая перечень программного обеспечения и информационных справочных систем

Лекционные аудитории, оснащенные мультимедийной техникой	Аудио-визуальная система лекционных аудиторий (мультимедийный проектор, экран, усилитель мощности звука, акустические системы, микрофоны, устройство коммутации, сетевой коммутатор для подключения к компьютерной сети (Интернет))	
Аудитории для проведения лабораторных и практических занятий	Ауд. №332а: комп. класс каф. ИнфБ, количество ПЭВМ-12 (компьютер Cjrei5-4570, ауд.№ 420: комп. класс каф. ИнфБ, количество ПЭВМ -12,(рабочая станция CPUCore 2DuoE6300 – 1.86), ауд. №424, комп класс каф. ИнфБ, количество ПЭВМ -12 (Компьютер Celeron D 2.8)	ОС Alt Linux (Альт Образование 8.2) Geany. Lazarus. Qt Creator. Quanta Plus. Веб-редактор Bluefish. Среда разработки Code::Blocks. Офисный пакет Libre Office 5.4: Base, Calc, Draw, Impress, Math, Writer. Пер- сональная бухгалтерия HomeBank. Словарь Star Dict. iTest. VM Max- ima. Кумир. Avidemux. Audacios. Brasero. Cheese. SMPlayer. Медиа-плеер Parole. Редактор тегов Easy TAG. Stath Studio. Pinta. Веб- браузер Mozilla Firefox. Графиче- ский редактор. FP – free Pascal. Microsoft Windows 7 (64 разрядная) Microsoft Office (standart) 2007; Microsoft Access 2007; Microsoft Project 2007; Microsoft Share Point 2007; Microsoft Visio 2007; Mi-

		crosoft SQL server 2008; 1 С Пред- приятие Лицензия; 7-Zip File Man- ager (архиватор); Adobe Acrobat Reader; Adobe Flash Player; FAR file manager; Google Chrome; Java TM 7 (64-bit); K-Lite Codec Pack; Mozilla Firefox; Oracle VM Virtu- alBox; Sublime Text; Symantec Endpoint Protection 12 (Заменен на AVP Kaspersky); VMWare Player; Антивирус “Зоркий глаз”; Lazarus; SmathStudio; NanoCAD; Gimp (графический редактор, аналог Photoshop); Avidemax (видео редактор); Virtual Dub (видео редактор); Free Pascal; Страж NT вер.3.0 Сертификат ФСТЭК № 2145 30.07.2013 г.; Ревизор 1XP Сертификат ФСТЭК № 989 08.02.2015 г.; Ревизор 2XP Сертификат ФСТЭК № 990 08.02.2015 г.; Фикс 2.0.2 Сертификат ФСТЭК №1548 15.01.2015 г.; Ревизор сети вер.3.0 Сертификат ФСТЭК №3413 02.06.2015 г.; СЗИ Панцирь К Сертификат ФСТЭК №1973 09.12.2015 г.; СЗИ Dallas Lock 8.0 К Сертификат ФСТЭК №2720 25.09.2015; СЗИ Dallas Lock 8.0 С Сертификат ФСТЭК №2945 16.08.2013
Аудитория для самостоятельной работы студентов (Читальные залы библиотеки)	Компьютеры со свободным доступом в сеть Интернет и Электронным библиотечным и информационно- справочным системам	
Аудитория для групповых и индивидуальных консультаций, текущего контроля и промежуточной аттестации	Комплекты мебели для учебного процесса – 30 шт., доска	

Аудитории для проведения занятий семинарского типа	Ауд. №332а: комп. класс каф. ИнфБ, количество ПЭВМ-12 (компьютер Core i5-4570, ауд.№ 420: комп. класс каф. ИнфБ, количество ПЭВМ -12,(компьютер Core i5-4460), ауд. №424, комп класс каф. ИнфБ, количество ПЭВМ -12 (Компьютер Регард РДЦБ)	ОС Alt Linux (Альт Образование 8.2) Geany. Lazarus. Qt Creator. Quanta Plus. Веб-редактор Bluefish. Среда разработки Code::Blocks. Офисный пакет Libre Office 5.4: Base, Calc, Draw, Impress, Math, Writer. Персональная бухгалтерия HomeBank. Словарь Star Dict. iTest. VM Max- ima. Кумир. Avidemux. Audacios. Brasero. Cheese. SMPlayer. Медиа-плеер Parole. Редактор тегов Easy TAG. Stath Studio. Pinta. Веб- браузер Mozilla Firefox. Графический редактор. FP – free Pascal.

При освоении дисциплины используется лицензионное и открытое программное обеспечение – *н-р, ОС Windows*

7 Материально-техническое обеспечение дисциплины (модуля)

Необходимый для реализации образовательной программы перечень материально-технического обеспечения включает:

- лекционные аудитории (оборудованные видеопроекционным оборудованием для презентаций; средствами звуковоспроизведения; экраном; имеющие выход в Интернет);
- помещения для проведения лабораторных и практических занятий (оборудованные учебной мебелью);
- библиотеку (имеющую рабочие места для студентов, оснащенные компьютерами с доступом к базам данных и Интернет);
- компьютерные классы.

Обеспеченность процесса обучения техническими средствами полностью соответствует требованиям ФГОС по специальности 10.05.03. Материально-техническая база приведена в лицензионных формах и расположена во внутренней сети по адресу http://education.vsuet.ru.

Аудитории для проведения лекционных, практических и лабораторных занятий, текущего контроля и промежуточной аттестации:

Учебная аудитория № 401 для проведения лекционных занятий, текущего контроля и промежуточной аттестации	Комплект мебели для учебного процесса – 80 шт. Переносной проектор Acer. Аудио-визуальная система лекционных аудиторий (мультимедийный проектор EpsonEB-X18, настенный экран ScreenMedia)	Microsoft Windows 8.1, Microsoft Office 2007 Standart, Microsoft Office 2007 Russian Academic OPEN No Level #44822753 от 17.11.2008 http://eopen.microsoft.com

Учебная аудитория. № 332а для проведения для проведения	Комплекты мебели для учебного процесса. ПЭВМ – 12 (компьютер Core i5-4570), стенды – 5 шт.	ОС Alt Linux (Альт Образование 8.2) Geany. Lazarus. Qt Creator. Quanta Plus. Веб-редактор Bluefish. Среда разработки Code::Blocks. Офисный пакет Libre Office 5.4: Base, Calc, Draw, Impress, Math, Writer. Персональная бухгалтерия HomeBank. Словарь Star Dict. iTest. VM Maxima. Кумир. Avidemux. Audacios. Brasero. Cheese. SMPlayer. Медиаплеер Parole. Редактор тегов Easy TAG. Stath Studio. Pinta. Веб-браузер Mozilla Firefox. Графический редактор. FP – free Pascal.

Аудитория для самостоятельной работы обучающихся, курсового и дипломного проектирования

Учебная аудитория № 424 для самостоятельной работы обучающихся, курсового и дипломного проектирования	Ауд. 424: Комплекты мебели для учебного процесса. ПЭВМ – 12: рабочая станция Регард РДЦБ.; стенды – 3	ОС Alt Linux (Альт Образование 8.2) Geany. Lazarus. Qt Creator. Quanta Plus. Веб-редактор Bluefish. Среда разработки Code::Blocks. Офисный пакет Libre Office 5.4: Base, Calc, Draw, Impress, Math, Writer. Персональная бухгалтерия HomeBank. Словарь Star Dict. iTest. VM Maxima. Кумир. Avidemux. Audacios. Brasero. Cheese. SMPlayer. Медиаплеер Parole. Редактор тегов Easy TAG. Stath Studio. Pinta. Веб-браузер Mozilla Firefox. Графический редактор. FP – free Pascal.

Дополнительно самостоятельная работа обучающихся может осуществляться при использовании:

Читальные залы библиотеки.	Компьютеры со свободным доступом в сеть Интернет и Электронными библиотечными и информационно справочными системами.	Microsoft Office Professional Plus 2010 Microsoft Open License Microsoft Office Professional Plus 2010 Russian Academic OPEN 1 License No Level #48516271 от17.05.2011 г. http://eooen.microsoft.com Microsoft Office 2007 Standart, Microsoft Open License Microsoft Office 2007 Russian Academic OPEN No Level #44822753 от 17.11.2008 http://eopen.microsoft.com Microsoft Windows XP, Microsoft Open License Academic OPEN No Level #44822753 от 17.11.2008 http://eopen.microsoft.com. Adobe Reader XI, (бесплатное ПО) httos://acrobat.adobe.com/ru/ru/acrobat/odfreader/volume-distribution.html

8 Оценочные материалы для промежуточной аттестации обучающихся по дисциплине (модулю)

Оценочные материалы (ОМ) для дисциплины (модуля) включают в себя:

- перечень компетенций с указанием индикаторов достижения компетенций, этапов их формирования в процессе освоения образовательной программы;
- описание шкал оценивания;
- типовые контрольные задания или иные материалы, необходимые для оценки знаний, умений, навыков;

- методические материалы, определяющие процедуры оценивания знаний, умений, навыков и (или) опыта деятельности.

ОМ представляются отдельным комплектом и **входят в состав рабочей программы дисциплины (модуля)**.

Оценочные материалы формируются в соответствии с П ВГУИТ «Положение об оценочных материалах».

ОЦЕНОЧНЫЕ МАТЕРИАЛЫ
ДЛЯ ПРОМЕЖУТОЧНОЙ АТТЕСТАЦИИ

по дисциплине

МЕТОДЫ И СРЕДСТВА КРИПТОГРАФИЧЕСКОЙ ЗАЩИТЫ ИНФОРМАЦИИ

1 Перечень компетенций с указанием этапов их формирования

№ п/п	Код компетенции	Формулировка компетенции	Код и наименование индикатора достижения компетенции
1	ОПК-10	способен использовать средства криптографической защиты информации при решении задач профессиональной деятельности;	ИД2$_{опк-10}$ – владеет методами и средствами криптографической защиты информации при решении задач профессиональной деятельности

Код и наименование индикатора достижения компетенции	Результаты обучения (показатели оценивания)
ИД2$_{опк-10}$ – владеет методами и средствами криптографической защиты информации при решении задач профессиональной деятельности	Знает: основные классы шифров, способы их реализации; программно-аппаратные средства реализации криптографических систем защиты информации; типовые поточные и блочные шифры, а также асимметричные криптосистемы; основные криптографические протоколы системы шифрования с открытыми ключами
	Умеет: : применять методы описания и исследования криптосистем; кодировать алгоритмы с соблюдением требований к качественному стилю программирования; определять структуру оптимальных устройств обработки сигналов информационных радиотехнических систем
	Владеет: навыками использования основных типов шифров и криптографических алгоритмов при решении задач обеспечения информационной безопасности; методами оценки криптографической стойкости алгоритмов шифрования; криптографической терминологией

2 Паспорт оценочных материалов по дисциплине

№ п/п	Разделы дисциплины	Индекс контролируемой компетенции (или ее части)	Оценочные материалы		Технология/процедура оценивания (способ контроля)
			наименование	№ заданий	
1	Организация криптографической передачи информации	ОПК-10	Тестовые задания	1-5	Бланочное или компьютерное тестирование
			Вопросы к зачету	83-94	Проверка преподавателем
			Вопросы к коллоквиуму	36-40	Проверка преподавателем
			Проработка материалов по лекциям, учебникам, учебным пособиям	26-27	Проверка преподавателем
2	Криптографические системы и их характеристики		Тестовые задания	6-10	Бланочное или компьютерное тестирование
			Вопросы к зачету	95-104	Проверка преподавателем
			Проработка материалов	28-29	Проверка преподавателем

			по лекциям, учебникам, учебным пособиям		
3	Реализация криптографических протоколов и алгоритмов		Банк тестовых заданий	11-15	Бланочное или компьютерное тестирование
			Кейс-задание	46-49	Защита практической работы
			Проработка материалов по лекциям, учебникам, учебным пособиям	30-31	Проверка преподавателем
			Вопросы к коллоквиуму	41-45	Проверка преподавателем
			Курсовая работа	65-82	Проверка препо-давателем
			Вопросы к экзамену	105-114	Проверка преподавателем

4	Блочные шифры. Поточное шифрование		Банк тестовых заданий	16-20	Бланочное или компьютерное тестирование
			Вопросы к экзамену	115-125	Проверка преподавателем
			Проработка материалов по лекциям, учебникам, учебным пособиям	32-33	Проверка преподавателем
			Реферат	30-44	Проверка преподавателем
5	Концептуальный подход к защите информации в компьютерных системах и сетях		Банк тестовых заданий	21-25	Бланочное или компьютерное тестирование
			Проработка материалов по лекциям, учебникам, учебным пособиям	34-35	Проверка преподавателем
			Вопросы к экзамену	126-133	Проверка преподавателем

3 Оценочные материалы для промежуточной аттестации.

Типовые контрольные задания или иные материалы, необходимые для оценки знаний, умений, навыков и (или) опыта деятельности, характеризующих этапы формирования компетенций в процессе освоения образовательной программы

Аттестация обучающегося по дисциплине проводится в форме тестирования и предусматривает возможность последующего собеседования (зачета).

Каждый вариант теста включает 20 контрольных заданий, из них:

- 7 контрольных заданий на проверку знаний;
- 7 контрольных заданий на проверку умений;
- 6 контрольных заданий на проверку навыков.

3.1 Тесты (тестовые задания к зачету)

3.1.1 ***Шифр и наименование*** **ОПК-10.** Способен использовать средства криптографической защиты информации при решении задач профессиональной деятельности;

№ задания	Тестовое задание с вариантами ответов и правильными ответами

1.	Криптографическая защита информации – это: 1. Защита информации, заключающаяся в обеспечении некриптографическими методами безопасности информации (данных), подлежащей (подлежащих) защите в соответствии с действующим законодательством, с применением технических, программных и программно-технических средств; **2. Защита информации с помощью ее криптографического преобразования;** 3. Защита информации путем применения организационных мероприятий и совокупности средств, создающих препятствия для проникновения или доступа неуполномоченных физических лиц к объекту защиты; 4. Защита информации правовыми методами, включающая в себя разработку законодательных и нормативных правовых документов (актов), регулирующих отношения субъектов по защите информации, применение этих документов (актов), а также надзор и контроль за их исполнением.
2.	Преобразование открытого текста сообщения в закрытый называется: **1. процедура шифрования;** 2. алгоритм шифрования; 3. обеспечение аутентификации; 4. цифровая запись
3.	Входные параметры процесса шифрования {несколько верных ответов): 1. зашифрованный текст; **2. ключ;** **3. открытый текст;** 4. алгоритм.
4.	Использование цифровой подписи позволяет не допустить (лишнее исключить): 1. Отказ от авторства. 2. Приписывание авторства. 3. Изменение содержания документа после подписания. 4. **Несанкционированное ознакомление с подписанным документом.**
5.	Отсутствие изменений в передаваемой или хранимой информации по сравнению с ее исходной записью – это **1. Целостность.** 2. Доступность. 3. Конфиденциальность. 4. Неотслеживаемость.
6.	Методы криптоанализа, использующие статистические характеристики открытых текстов, наиболее эффективны при анализе: **1. Шифров замены.** 2. Шифров перестановки. 3. Шифров гаммирования. 4. Композиционных шифров
7.	Иностранным аналогом стандарта ГОСТ 28147-89 является: 1. Алгоритм А5. **2. Алгоритм DES.** 3. Алгоритм Гиффорда. 4. Алгоритм Adler-32
8.	Шифр простой замены - это: 1. Шифр, в котором каждый элемент открытого текста преобразуется элемент шифрованного текста с использованием нескольких алфавитов. 2. Шифр, в котором ключом шифрования служит достаточно большое число. **3. Шифр, в котором каждый элемент открытого текста преобразуется в элемент шифрованного текста с использованием одного и того же алфавита.** 4. Шифр, который дешифруется достаточно просто.
9.	Под энтропией в криптографии понимается: **1. Количество информации на символ передаваемого сообщения.** 2. Мера неопределенности передаваемого сообщения. 3. Количество информации, содержащейся в целом передаваемом сообщении. 4. Количество символов текста, которое возможно передать в единицу времени.

10.	Набор правил и процедур, предназначенный для выполнения функций криптографической системы, в процессе которого участники используют криптографические алгоритмы: 1. Криптографический алгоритм. **2. Криптографический протокол.** 3. Криптографическая система. 4. Криптографический ключ.
11.	Криптосистемы RSA и Эль-Гамаля относятся к: 1. Шифрам перестановки. **2. Асимметричным.** 3. Композиционным. 4. Симметричным
12.	Какой из режимов алгоритма DES используется для построения шифров гаммирования? 1. электронная кодовая книга; 2. сцепление блоков шифра; 3. обратная связь по шифротексту; **4. обратная связь по выходу**
13.	Количество последовательностей, из которых состоит расшифровка текста по таблице Вижинера: **1. 3** 2. 4 3. 5
14.	Процесс, выполняемый после создания сеансового ключа DES: 1. Подписание ключа 2. Передача ключа на хранение третьей стороне 3. Кластеризация ключа **4. Обмен ключом**
15.	Определение фактора трудозатрат для алгоритма 1. Время зашифрования и расшифрования открытого текста **2. Время, которое займет взлом шифрования** 3. Время, которое занимает выполнение 16 циклов преобразований 4. Время, которое занимает выполнение функций подстановки
16.	Функция Эйлера, используемая в вычислении открытого и закрытого ключей шифрования в алгоритме RSA, вычисляется по формуле: 5. (p-1)*(N-1). **6. (p-1)*(q-1).** 7. (N-1)*(q-1). 8. (N*q)+(N*p)
17.	Способность шифра противостоять попыткам противника по имитации или подмене называется 1. Неизменность. **2. Имитостойкость.** 3. Секретность. 4. Неотслеживаемость
18.	Какие операции применяются обычно в современных блочных алгоритмах симметричного шифрования? (несколько) 1. Возведение в степень **2. замена бит по таблице замен** 3. нахождение остатка от деления на большое простое число 4. **перестановка бит** 5. **сложение по модулю 2**
19.	Алгоритм ГОСТ 28147-89 является **1. блочным алгоритмом симметричного шифрования** 2. алгоритмом формирования электронной цифровой подписи 3. блочным алгоритмом асимметричного шифрования 4. алгоритмом вычисления функции хеширования
20.	На сколько блоков будет разбито сообщение размером 1 Кбайт для шифрования алгоритмом по ГОСТ 28147-89?Ответ запишите в виде одного числа **Ответ: 128**

21.	Что такое защита информации? 1. Состояние защищенности национальных интересов в информационной сфере, определяющихся совокупностью сбалансированных интересов личности, общества и государства. 2. Реализация конституционных прав человека и гражданина на доступ к информации, на использование информации в интересах осуществления не запрещенной законом деятельности, физического, духовного и интеллектуального развития, а также защита информации, обеспечивающая личную безопасность. 3. Деятельность, направленная на предотвращение НСД к информации. **4. Деятельность, направленная на предотвращение утечки защищаемой информации, непреднамеренных и несанкционированных воздействий на защищаемую информацию.**
22.	Структурная комплексность включает: 1. обеспечение маскировки (скрытия) назначения, архитектуры, технологии функционирования системы; 2. обеспечение текущей защиты, обеспечение защиты на заданном интервале времени, обеспечение защиты на всех этапах жизненного цикла; **3. защиту информации в элементах и отдельных средствах, защиту информации в отдельно взятой системе обработки информации, защиту информации в системах обработки информации страны, региона, ведомства;** 4. комплексный учет концепций развития и использования современных средств обработки информации, учет аспектов системности подхода.
23.	Концептуальная комплексность включает: 1. обеспечение маскировки (скрытия) назначения, архитектуры, технологии функционирования системы; 2. обеспечение текущей защиты, обеспечение защиты на заданном интервале времени, обеспечение защиты на всех этапах жизненного цикла; 3. защиту информации в элементах и отдельных средствах, защиту информации в отдельно взятой системе обработки информации, защиту информации в системах обработки информации страны, региона, ведомства; **4. комплексный учет концепций развития и использования современных средств обработки информации, учет аспектов системности подхода.**
24.	Чем определяется уровень надежности применяемых криптографических преобразований: **1) значением допустимой вероятности неисправностей или сбоев, приводящих к получению злоумышленником дополнительной информации о криптографических преобразованиях;** 2) сложностью комбинации символов, выбранных случайным образом; 3) использованием большого числа ключей для шифрования; 4) отношением количества дешифрованной информации к общему количеству шифрованной информации, подлежащей дешифрованию.
25.	Ниже перечислены механизмы защиты информационных систем от несанкционированного доступа. Что здесь лишнее: 1) идентификация и аутентификация пользователей и субъектов доступа; 2) управление доступом; **3) обеспечение постоянного числа пользователей сети;** 4) обеспечения целостности; 5) регистрация и учет.

3.2 Проработка материалов по лекциям, учебникам, учебным пособиям

Вопросы

3.2.1 Шифр и наименование компетенции **ОПК-10.** Способен использовать средства криптографической защиты информации при решении задач профессиональной деятельности;

№ задания	Текст вопроса (задачи, задания)
26.	Свойства простых шифров
27.	Стенографические методы защиты информации

28.	Шифры замены
29.	Совершенные шифры
30.	Криптосистема RSA
31.	Принципы построения алгоритмов
32.	Принципы построения блочных шифров
33.	Имитация и подмена сообщения
34.	Свойства псевдослучайных последовательностей
35.	Криптографические хеш-функции

3.3 Вопросы к коллоквиуму

Вопросы для экзамена

3.3.1 Шифр и наименование компетенции **ОПК-10.** Способен использовать средства криптографической защиты информации при решении задач профессиональной деятельности;

№ задания	Текст вопроса (задачи, задания)
36.	Классификация систем шифрования
37.	Симметричное шифрование, достоинства и недостатки.
38.	Асимметричное шифрование, достоинства и недостатки
39.	Основы симметричного шифрования.
40.	Блочные криптоалгоритмы
41.	Сеть Фейштеля
42.	Математические основы шифрования с открытым ключом
43.	Современные поточные шифры
44.	Стенография. Основные понятие
45.	Основные методы криптоанализа

3.4 Кейс-задания

3.4.1 ***Шифр и наименование компетенции*** **ОПК-10.** Способен использовать средства криптографической защиты информации при решении задач профессиональной деятельности;

№ задания	Текст задания

46.	Используя аффинный мультипликативный алгоритм с ключом P[7] (по модулю 26), зашифровать сообщение “hello” **Решение** **Ключ должен быть в Z_{26*}. Это множество имеет только 12 элементов: 1, 3, 5, 7, 9, 11, 15, 17, 19, 21, 23, 25.** **Мы используем мультипликативный шифр, чтобы зашифровать сообщение "hello" с ключом 7. Зашифрованный текст "XCZZU".** **Исходный текст h 07Шифрование (07 x 07) mod 26 Шифр. Текст 23 X** **Исходный текст e 04Шифрование (04 x 07) mod 26 Шифр. Текст 02 C** **Исходный текст l 11Шифрование (11 x 07) mod 26 Шифр. Текст 25 Z** **Исходный текст l 11Шифрование (11 x 07) mod 26 Шифр. Текст 25 Z** **Исходный текст o 14Шифрование (14 x 07) mod 26 Шифр. Текст 20 U**
47.	Определите ключи шифра Цезаря, если известны следующая пара: открытый текст — шифротекст: ВИНОГРАД — ШЯДЕЩЖЦЪ (исходный алфавит: АБВГДЕЕЁЖЗИЙКЛМНОПРСТУФХЦЧШЩЪЫЬЭЮЯ) **Ответ:** **Ключ – 23**
48.	Пусть исходный алфавит состоит из следующих знаков – «АБВГДЕЖЗИЙКЛМНОПРСТУФХЦУЧШЩЪЫЬЭЮЯ». Расшифруйте сообщение «УИЯД БРЗЪНЮПЮИ ТАТСЮНЫ», зашифрованное с помощью таблицы Вижнера и ключа «ВГУИТ» **Ответ: «С НОВЫМ ГОДОМ»**
49.	Пусть исходный алфавит состоит из следующих знаков – «АБВГДЕЖЗИКЛМНОПРСТУФХЦУЧШЩЪЫЬЭЮЯ». Зашифруйте сообщение «науки юношей питают отраду старым подают» с помощью шифра Атбаш. **Ответ: Уянцч бутзъй счоябо, торяын поярдф стыябо**

3.5 Реферат

3.5.1 ***Шифр и наименование компетенции*** **ОПК-10.** Способен использовать средства криптографической защиты информации при решении задач профессиональной деятельности;

№ задания	Текст вопроса (задачи, задания)
50	Щифр Цезаря. Аффинные криптосистемы.
51	Векторный шифр Аббата Тритемиуса.
52	Шифрующие матрицы. Матричные криптосистемы.
53	Криптосистема с открытым ключом. Алгоритм RSA.
54	Циклическая атака на алгоритм RSA.
55	Электронная цифровая подпись и хэш-функция.
56	Эллиптические кривые. Сложение точек эллиптической кривой.
57	Криптосистемы на эллиптических кривых.
58	Определение шифра.
59	Определение ключа.
60	Определение криптосистемы.
61	Определение совершенного шифра по Шеннону.
62	Теоретическая мера стойкости шифра, расстояние единственности.

63	Алгебраическая модель шифра простой замены.
64	Признак, по которому производится классификация шифров. Общая классификация шифров.

3.6 Курсовая работа

3.6.1 ***Шифр и наименование компетенции*** **ОПК-10.** Способен использовать средства криптографической защиты информации при решении задач профессиональной деятельности;

№ задания	Текст вопроса (задачи, задания)
65	Разработка алгоритма и программы исследования корреляционных свойств криптографических примитивов
66	Разработка алгоритма и программы по исследованию статистических свойств блочных алгоритмов шифрования
67	Разработка алгоритма и программы разложения целых чисел для анализа шифра RSA
68	Разработка алгоритма и программы по линейному анализу криптографических примитивов и блочных шифров
69	Разработка и реализация программного комплекса для исследования свойств криптографических ключей
70	Разработка алгоритма и программы по анализу шифра AES
71	Разработка программного комплекса анализа VPN
72	Разработка алгоритма и программы реализации и исследованию свойств хэш-функций
73	Разработка алгоритма и программы криптоанализа систем на эллиптических кривых по методу Полларда
74	Разработка алгоритма анализа шифра AES в соответствии с алгебраическим методом
75	Разработка алгоритмов анализа свойств нелинейных подстановок на основе дискретных преобразований
76	Разработка алгоритма и программы разложения целых чисел на основе метода решета числового поля
77	Разработка алгоритма и программы анализа подстановок большой размерности
78	Разработка алгоритма и программы визуального проектирования блочных шифров
79	Программная реализация алгоритмов блочного шифрования данных для устройств, функционирующих под управлением ОС Android
80	Применение криптографических алгоритмов для защищенной организации систем дистанционного обучения
81	Разработка алгоритма и программы генерации больших чисел
82	Разработка алгоритма и программы выбора эллиптических кривых для системы цифровой электронной подписи и аутентификации

3.7 Зачет (собеседование)

Вопросы для зачета

3.7.1 Шифр и наименование компетенции **ОПК-10.** Способен использовать средства криптографической защиты информации при решении задач профессиональной деятельности;

№ задания	Текст вопроса (задачи, задания)
83	Признак, по которому производится классификация шифров.
84	Общая классификация шифров.
85	Математическая модель шифров простой замены.
86	Математическая модель шифров перестановки.

87	Классификация шифров замены.
88	Классификация шифров перестановки.
89	Существуют ли шифры, не являющиеся ни шифрами замены, ни шифрами перестановки?
90	Определение шифра табличного гаммирования.
91	Определение шифра модульного гаммирования.
92	Почему недопустимо использовать дважды одну и ту же гамму (даже случайную и равновероятную) для зашифрования разных открытых текстов?
93	Почему наложение на открытый текст гаммы, представляющей собой периодическую последовательность небольшого периода, не дает надежной защиты?
94	Определение криптосистемы с открытым ключем (асимметричной криптосистемы).
95	Обобщенная схема асимметричной криптосистемы с открытым ключом.
96	Характерные особенности асимметричных криптосистем.
97	Требования, выполнение которых обеспечивает безопасность асимметричной криптосистемы.
98	Определение однонаправленной функции.
99	Перечислите шифрсистемы с открытым ключом.
100	На чем основана стойкость шифрсистемы RSA ?
101	На чем основана стойкость шифрсистемы Эль гамаля ?
102	На чем основана стойкость шифрсистемы Мак Элиса ?
103	Сущность аттестования компьютерных систем.
104	Чем определяется надежность защиты информации в компьютерной системе.

3.8 Экзамен (собеседование)

Вопросы для экзамена

3.8.1 Шифр и наименование компетенции **ОПК-10.** Способен использовать средства криптографической защиты информации при решении задач профессиональной деятельности;

№ задания	Текст вопроса (задачи, задания)
105	Как определяются энтропия и избыточность языка?
106	Как можно качественно охарактеризовать избыточность языка?
107	Какие тексты на русском языке имеют большую избыточность: литературные или технические
108	Почему неопределенность шифра по открытому тексту (или по ключу) можно рассматривать как меру теоретической стойкости шифра?
109	Как зависит расстояние единственности для шифра от энтропии языка?
110	Найдите расстояние единственности для шифра Виженера, который используется для шифрования русских технических текстов с избыточностью 0,8.
111	Дайте определение совершенного шифра
112	Практическая стойкость шифра. Рабочая характеристика шифра.
113	Что такое имитостойкость шифра?
114	Что может служить мерой имитостойкости шифра?
115	Является ли шифр гаммирования имитостойким?
116	Что такое совершенная имитостойкость шифра?

117	Является ли шифр гаммирования шифром, не размножающим искажений типа "замена знаков", искажения типа "пропуск знаков"?
118	Дайте определение кода.
119	Что такое кодовое расстояние по Хэммингу?
120	Какие классы кодов вы знаете?
121	Чем отличаются блоковые и древовидные коды?
122	Какое количество ошибок может исправить блоковый код?
123	Чем отличаются полные и неполные декодеры?
124	Свойства псевдослучайных последовательностей на основе ЛРР.
125	Преимущества и недостатки перехода к шифрованию сообщений в алфавитах большой мощности.
126	Реализация принципа "перемешивания" при практической реализации алгоритмов блочного шифрования.
127	Достоинства и недостатки систем поточного шифрования по сравнению с блочными шифрами.
128	Синхронизации поточных шифров.
129	Функции управляющего блока.
130	Функции шифрующего блока.
131	За счет чего можно обеспечить стойкость алгоритма шифрования при повторном использовании ключей?
132	Достоинства линейных регистров сдвига, используемых в качестве управляющих блоков поточных шифрсистем?
133	Особенности программной реализации функций защиты информации КС.

4. Методические материалы, определяющие процедуры оценивания знаний, умений, навыков и (или) опыта деятельности, характеризующих этапы формирования компетенций

Процедуры оценивания в ходе изучения дисциплины знаний, умений и навыков, характеризующих этапы формирования компетенций, регламентируются положениями:

- П ВГУИТ 2.4.03 Положение о курсовых экзаменах и зачетах;
- П ВГУИТ 4.1.02 Положение о рейтинговой оценке текущей успеваемости, а также методическими указаниями.

Итоговая оценка по дисциплине определяется на основании определения средневзвешенному значения баллов по каждому заданию.

5. Описание показателей и критериев оценивания компетенций на различных этапах их формирования, описание шкал оценивания для каждого результата обучения по дисциплине/практике

Результаты обучения по этапам формирования компетенций	Предмет оценки (продукт или процесс)	Показатель оценивания	Критерии оценивания сформированности компетенций	Шкала оценивания	
				Академическая оценка или баллы	Уровень освоения компетенции
Шифр и наименование компетенции **ОПК-10.** Способен использовать средства криптографической защиты информации при решении задач профессиональной деятельности;					
ЗНАТЬ: основные классы шифров, способы их реализации; программно-аппаратные средства реализации криптографических систем защиты информации; типовые поточные и блочные шифры, а также асимметричные криптосистемы; основные криптографические протоколы системы шифрования с открытыми ключами	Собеседование (зачет)	Уровень знаний	50% и более правильных ответов	Зачтено	Освоена (базовый, повышенный)
			менее 50% правильных ответов	Не зачтено	Не освоена (недостаточный)
УМЕТЬ: определять уязвимые места информационных автоматизированных систем, разрабатывать регламент тестирования защищенных автоматизированных систем	Тест (тестовые задания к зачету)	Умение применять полученные знания	85% и более правильных ответов	Отлично	Освоена (повышенный)
			75-84% правильных ответов	Хорошо	Освоена (повышенный)
			65-74% правильных ответов	Удовлетворительно	Освоена (базовый)
			Менее 64% правильных ответов	Неудовлетворительно	Не освоена (недостаточный)
ВЛАДЕТЬ: навыками выявления нарушения защищенности автоматизированных систем, навыками администрирования и	Кейс-задание	Методика и правильность решения задачи	Обучающийся разобрался в предложенной конкретной ситуации, самостоятельно решил поставленную задачу на основе полученных знаний	Зачтено	Освоена (базовый, повышенный)
			Обучающийся не разобрался в сложившейся ситуации, не выявил	Не зачтено	Не освоена (недостаточный)

управления инструментальными средствами в области информационной безопасности			причины случившегося и не предложил вариантов решения		