Минобрнауки России
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

РАБОЧАЯ ПРОГРАММА ДИСЦИПЛИНЫ

Криптографические протоколы и стандарты

Специальность

10.05.03 Информационная безопасность автоматизированных систем

Специализация

Безопасность открытых информационных систем

Квалификация выпускника

специалист по защите информации

1. Цели и задачи дисциплины

Целями и задачами дисциплины «Криптографические протоколы и стандарты» в соответствии с видами профессиональной деятельности являются:

- проведение инструментального мониторинга защищенности автоматизированных систем и анализа его результатов;
- выполнение проектов по созданию программ, комплексов программ, программноаппаратных средств, баз данных, компьютерных сетей для защищенных автоматизированных систем.

Объектами профессиональной деятельности являются:

– автоматизированные системы, функционирующие в условиях существования угроз в информационной сфере и обладающие информационно-технологическими ресурсами, подлежащими защите;

– информационные технологии, формирующие информационную инфраструктуру в условиях существования угроз в информационной сфере и задействующие информационно-технологические ресурсы, подлежащие защите;

– технологии обеспечения информационной безопасности автоматизированных систем;

– системы управления информационной безопасностью автоматизированных систем.

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

В результате освоения дисциплины в соответствии с предусмотренными компетенциями обучающийся должен:

№ п/п	Код компетенции	Содержание компетенции (результат освоения)	В результате изучения учебной дисциплины обучающийся должен:		
			знать	уметь	владеть
1	ОПК-3	способностью применять языки, системы и инструментальные средства программирования в профессиональной деятельности	основные подходы к автоматизации криптографических протоколов	применять протоколы привязки к биту на основе дискретного логарифмирования	навыками распределения ключа при наличии доверенного центра
2	ПК-14	способностью проводить контрольные проверки работоспособности применяемых программно-аппаратных, криптографических и технических средств защиты информации	типовые криптографические протоколы и основные требования к ним, принципы построения криптографических хеш-функций; протоколы идентификации, протоколы передачи и распределения ключей	использовать симметричные и ассиметричные шифросистемы для построения криптографических протоколов, проводить сравнительный анализ криптографических протоколов	навыками систематизации научно-технической информации в сфере криптографической защиты информации

3. Место дисциплины в структуре ОП ВО

Дисциплина «Криптографические протоколы и стандарты» относится к блоку 1 ОП и ее базовой части.

Изучение дисциплины основано на знаниях, умениях и навыках, полученных при изучении обучающимися дисциплин:

- Языки программирования;
- Криптографические протоколы и стандарты;
- Учебная практика, практика по получению первичных профессиональных умений;
- Технологии и методы программирования;
- Система обнаружения компьютерных атак.

Дисциплина является предшествующей для изучения дисциплин, прохождения практик:

- Мультимедиатехнологии;
- Криптографические методы защиты информации;
- Производственная практика, практика по получению профессиональных умений и опыта профессиональной деятельности;
- Производственная практика, преддипломная практика;

защиты выпускной квалификационной работы, включая подготовку к процедуре защиты и процедуру защиты.

4. Объем дисциплины и виды учебных занятий

Общая трудоемкость дисциплины составляет 5 зачетных единиц.

Виды учебной работы	Всего часов	Семестр
		6
	акад ч.	**акад. ч**
Общая трудоемкость дисциплины	**180**	**180**
Контактная работа, в т.ч. аудиторные занятия	**76**	**76**
Лекции	36	36
в том числе в форме практической подготовки	–	–
Практические занятия (ПЗ)	36	36
в том числе в форме практической подготовки	36	36
Консультации текущие	1,8	1,8
Проведение консультаций перед экзаменом	2	2
Вид аттестации – экзамен	0,2	0,2
Самостоятельная работа	**70,2**	**70,2**
Подготовка доклада с презентацией	10	10
Подготовка к коллоквиуму	15	15
Домашнее задание	25	25
Курсовая работа	20,2	20,2
Подготовка к экзамену (контроль)	**33,8**	**33,8**

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

5.1 Содержание разделов дисциплины

№ п/п	Наименование разделов дисциплины	Содержание раздела	Трудоемкость раздела, час
1	Понятие криптографического протокола	Роль криптографических протоколов в системах защиты информации. Понятие криптографического протокола. Свойства протоколов, характеризующие их	21

		безопасность. Основные виды уязвимостей. Подходы к классификации криптографических протоколов. Подходы к моделированию криптографических протоколов. Понятие уязвимости и атаки на криптографический протокол. Использование симметричных и асимметричных шифрсистем для построения криптографических протоколов. Примеры. Основные подходы к автоматизации анализа протоколов	
2	Привязка к биту и электронная жеребьевка	Вычислительная и безусловная связанность, секретность. Блоб. Протоколы привязки к биту на основе проблемы дискретного логарифмирования, на основе симметричной криптосистемы, на основе односторонней функции, односторонней перестановки.	21
3	Разделение секрета. Прикладные протоколы.	Понятие схемы разделения секрета (СРС). Группа доступа. Структура доступа. Пороговые СРС – схема Шамира, схема Блекли, схема на основе Китайской теоремы об остатках. Разделение секрета для произвольной группы доступа. Совершенная СРС. Идеальное разделение секрета. Проверяемое разделение секрета. Протоколы конфиденциальных вычислений. Пример для схемы Шамира.	27
4	Протоколы идентификации с нулевым разглашением. Протоколы открытых сделок	Понятие об интерактивных системах доказательства (ИСД). Примеры ИСД (квадратичные невычеты; неизоморфизм графов). Примеры ИСД с нулевым разглашением (изоморфизм графов). Вопросы реализации ИСД. Нулевое разглашение припараллельной композиции раундов. Схема Фиата-Шамира. Схема Файге-Фиата Шамира. Схема Шнорра. Схема Брикелла-МакКарли. Схема Окамото и теорема о ее условной стойкости. Схема Гиллу-Кискатр. Доказательства полноты и корректности этих схем. Слепая подпись. Затемненная подпись. Применение слепых подписей. Скрытый канал. Подписи со скрытым каналом. Скрытый канал на основе подписи Онга-ШнорраШамира. Подход к построению скрытого канала. Подписи, свободные от скрытого канала. Покер по телефону. Электронная монета и электронные платежи. Протоколы голосования. Протоколы установления подлинности.	27
5	Построение криптографических хеш-функций. Инфраструктура открытых ключей.	Управление открытыми ключами. Основы организации и основные компоненты инфраструктуры открытых ключей. Сертификат открытого ключа. Стандарт X.509. Сервисы инфраструктуры откры-	27

		тых ключей. Удостоверяющий центр. Центр регистрации. Репозиторий. Архив сертификатов. Конечные субъекты. Архитектуры инфраструктуры открытых ключей. Проверка и отзыв сертификата открытого ключа. Этапы жизненного цикла ключей	
6	Управление ключами.	Задачи управления ключами, решаемые криптографическими средствами. Централизованная выработка ключа. Совместная выработка ключа. Распределение ключа при наличии доверенного центра. Распределение секретного ключа без участия доверенного центра. Схемы Wide-Mouth Frog, Yahalom, протокол Нидхема-Шредера, ОтвеяРииса. Бесключевой протокол Шамира. Протокол ДиффиХэллмана. Протокол Нидхема-Шредера на основе шифра с открытым ключом. Широковещательное распределение ключей. Протокол Kerberos	19,2

5.2 Разделы дисциплины и виды занятий

№ п/п	Наименование раздела дисциплины	Лекции, час	ПЗ, час	СР, час
1	Понятие криптографического протокола	6	6	9
2	Привязка к биту и электронная жеребьевка	6	6	9
3	Разделение секрета. Прикладные протоколы	6	6	15
4	Протоколы идентификации с нулевым разглашением. Протоколы открытых сделок	6	6	15
5	Построение криптографических хеш-функций. Инфраструктура открытых ключей. Управление ключами	6	6	15
6	Управление ключами	6	6	7,2

5.2.1 Лекции

№ п/п	Наименование раздела дисциплины	Тематика лекционных занятий	Трудоемкость, Час
1	Понятие криптографического протокола	Роль криптографических протоколов в системах защиты информации. Понятие криптографического протокола. Свойства протоколов, характеризующие их безопасность. Основные виды уязвимостей. Подходы к классификации криптографических протоколов. Подходы моделированию криптографических протоколов. Понятие уязвимости и атаки на криптографический протокол. Использование симметричных и асимметричных шифрсистем для построения криптографических протоколов. Примеры. Основные подходы к автоматизации анализа протоколов.	6
2	Привязка к биту и электронная жеребьевка	Вычислительная и безусловная связанность, секретность. Блоб. Протоколы привязки к биту на основе проблемы дискретного логарифмирования, на основе симметричной	6

		криптосистемы, на основе односторонней функции, односторонней перестановки.	
3	Разделение секрета. Прикладные протоколы	Понятие схемы разделения секрета (СРС). Группа доступа. Структура доступа. Пороговые СРС – схема Шамира, схема Блекли, схема на основе Китайской теоремы об остатках. Разделение секрета для произвольной группы доступа. Совершенная СРС. Идеальное разделение секрета. Проверяемое разделение секрета. Протоколы конфиденциальных вычислений. Пример для схемы Шамира.	6
4	Протоколы идентификации с нулевым разглашением. Протоколы открытых сделок	Понятие об интерактивных системах доказательства (ИСД). Примеры ИСД (квадратичные невычеты; неизоморфизм графов). Примеры ИСД с нулевым разглашением (изоморфизм графов). Вопросы реализации ИСД. Нулевое разглашение при параллельной композиции раундов. Схема ФиатаШамира. Схема Файге-Фиата-Шамира. Схема Шнорра. Схема Брикелла-МакКарли. Схема Окамото и теорема о ее условной стойкости. Схема Гиллу-Кискатр. Доказательства полноты и корректности этих схем. Слепая подпись. Затемненная подпись. Применение слепых подписей. Скрытый канал. Подписи со скрытым каналом. Скрытый канал на основе подписи Онга-Шнорра-Шамира. Подход к построению скрытого канала. Подписи, свободные от скрытого канала. Покер по телефону. Электронная монета и электронные платежи. Протоколы голосования. Протоколы установления подлинности.	6
5	Построение криптографических хеш-функций. Инфраструктура открытых ключей. Управление ключами	Управление открытыми ключами. Основы организации и основные компоненты инфраструктуры открытых ключей. Сертификат открытого ключа. Стандарт X.509. Сервисы инфраструктуры открытых ключей. Удостоверяющий центр. Центр регистрации. Репозиторий. Архив сертификатов. Конечные субъекты. Архитектуры инфраструктуры открытых ключей. Проверка и отзыв сертификата открытого ключа. Этапы жизненного цикла ключей.	6
6	Управление ключами	Задачи управления ключами, решаемые криптографическими средствами. Централизованная выработка ключа. Совместная выработка ключа. Распределение ключа при наличии доверенного центра. Распределение секретного ключа без участия доверенного центра. Схемы Wide-Mouth Frog, Yahalom, протокол Нидхема-Шредера, ОтвеяРииса. Бесключевой протокол Шамира. Протокол Диффи-Хэллмана. Протокол Нидхема-Шредера на основе шифра с открытым ключом. Широковещательное распределение ключей. Протокол Kerberos.	6

5.2.2 Практические занятия

№ п/п	Наименование раздела дисциплины	Тематика практических занятий	Трудоемкость, час
1	Понятие криптографического протокола	№ 1. Анализ безопасности простейших протоколов. Классификация атак. № 2. Анализ протоколов цифровых подписей. Анализ DSA и ГОСТ.	6
2	Привязка к биту и электронная жеребьевка	№ 3. Компьютерная реализация схем электронной жеребьевки и привязки к биту.	6
3	Разделение секрета. Прикладные протоколы	№ 4. Реализация пороговых схем разделения секрета и СРС для произвольной структуры доступа. № 5. Проверяемое разделение секрета и конфиденциальные вычисления № 6. Протоколы семейства KriptoKnight для различных сетевых конфигураций и условий применения. № 7. Протоколы семейства IP-Sec.	6
4	Протоколы идентификации с нулевым разглашением. Протоколы открытых сделок	№ 8. Парольные схемы. Одноразовые пароли. № 9. Схемы рукопожатия № 10. Интерактивные системы доказательства. № 11. Имитационное моделирование протоколов идентификации на основе ИСД с нулевым разглашением.	6
5	Построение криптографических хеш-функций. Инфраструктура открытых ключей. Управление ключами	№ 12. Компьютерная реализация схем слепой подписи и скрытого канала. Компьютерная реализация протокола «Покер по телефону» для 3х игроков. № 13. Имитационное моделирование схемы электронных денег с монетами одинакового достоинства.	6
6	Управление ключами	№ 14. Изучение работы с удостоверяющим центром при помощи CryptoPro. № 15. Формирование и проверка сертификата с использованием CryptoPro. № 16. Компьютерная реализация протокола передачи секретного ключа через доверенный центр (работа в группах). № 17. Компьютерная реализация протокола передачи секретного ключа средствами асимметричной криптографии (работа в группах).	6

5.2.3 Лабораторный практикум Не предусмотрен

5.2.4 Самостоятельная работа обучающихся (СРО)

№ п/п	Наименование раздела дисциплины	Вид СРО	Трудоемкость, час
1	Управление ключами	Тестирование	7,2
2	Понятие криптографического протокола		9
3	Привязка к биту и электронная жеребьевка		9
4	Разделение секрета. Прикладные протоколы	Подготовка доклада с визуальным представлением	15
5	Протоколы идентификации с нулевым разглашением. Протоколы открытых сделок	Расчетно-практическая работа «Построение криптографических хеш-функций»	15
6	Построение криптографических хеш-функций. Инфраструктура открытых ключей. Управление ключами		15

6 Учебно-методическое и информационное обеспечение дисциплины

1.1 Основная литература

1.Криптографические методы и средства защиты информации [Текст] : учебное пособие для студ. по направлению "Информационная безопасность" / Н. Г. Бутакова, Н. Федоров. СПб. : ИЦ "Интермедия", 2016. 384 с. ISBN 978-5-43830135-6 : 622-00 http://biblos.vsuet.ru/MegaPro/Web/SearchResult/MarcFormat/99425

2.Основы криптографии [Текст] : учебное пособие для обучающихся по направлению подготовки бакалавров и магистров: 10.04.01, 10.03.01, 43.03.01,11.03.02,11.04.02 и спец. 210403 / В. И. Коржик, В. А. Яковлев. СПб. : ИЦ Интермедия, 2016. – 296 с. ISBN 978-5-89160-097-3: 822-00 http://biblos.vsuet.ru/MegaPro/Web/SearchResult/MarcFormat/99427

3. Основы криптографии [Текст] : учебное пособие для обуч. по направлению подготовки бакалавров и магистров: 10.04.01, 10.03.01, 43.03.01,11.03.02,11.04.02 и спец. 210403 / В. И. Коржик, В. А. Яковлев. СПб. : ИЦ Интермедия, 2016. 296 с. ISBN 978-5-89160-097-3 : 822-00 http://biblos.vsuet.ru/MegaPro/Web/SearchResult/MarcFormat/99427

6.2. Дополнительная литература

1. Семенов, Ю. А. Алгоритмы телекоммуникационных сетей. В 3 частях. Часть 1. Алгоритмы и протоколы каналов и сетей передачи данных / Ю.А. Семенов. М.: Интернет-университет информационных технологий, Бином. Лаборатория знаний, 2016. – 640 с.

2. Жданов, О. Н. Методика выбора ключевой информации для алгоритма блочного шифрования / О.Н. Жданов. М.: ИНФРА-М, 2015. – 869 с.

3. Стохастические методы и средства защиты информации в компьютерных системах и сетях: моногр. / Под редакцией И.Ю. Жукова. М.: КУДИЦ-Пресс, 2016. – 512 с.

4. Столлингс, В. Компьютерные сети, протоколы и технологии Интернета / В. Столлингс. М.: БХВ-Петербург, 2014. – 506 с.

5. Ищукова, Е.А. Криптографические протоколы и стандарты : учебное пособие / Е.А. Ищукова, Е.А. Лобова ; Министерство образования и науки РФ, Южный федеральный университет, Инженернотехнологическая академия. – Таганрог : Издательство Южного федерального университета, 2016. – 80 с.

6.3 Перечень учебно-методического обеспечения для самостоятельной работы обучающихся

Криптографические методы защиты информации [Электронный ресурс]: 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, 2016. – 20 с. http://biblos.vsuet.ru/ProtectedView/Book/ViewBook/

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

Наименование ресурса сети «Интернет»	Электронный адрес ресурса
«Российское образование» федеральный портал	*https://www.edu.ru/*
Научная электронная библиотека	*https://elibrary.ru/defaultx.asp*
Национальная исследовательская компьютерная сеть России	*https://niks.su/*
Информационная система «Единое окно доступа к образовательным ресурсам»	*http://window.edu.ru/*
Электронная библиотека ВГУИТ	*http://biblos.vsuet.ru/megapro/web*
Сайт Министерства науки и высшего образования РФ	*https://minobrnauki.gov.ru/*
Портал открытого on-line образования	*https://npoed.ru/*
Электронная информационно-образовательная среда ФГБОУ ВО «ВГУИТ»	*https://education.vsuet.ru/*

6.5 Методические указания для обучающихся по освоению дисциплины

Методические указания для обучающихся по освоению дисциплин (модулей) в ФГБОУ ВО ВГУИТ [Электронный ресурс] : методические указания для обучающихся на всех уровнях высшего образования / М. М. Данылив, Р. Н. Плотникова; ВГУИТ, Учебно-методическое управление. Воронеж : ВГУИТ, 2016. – Режим доступа : http://biblos.vsuet.ru/MegaPro/Web/SearchResult/MarcFormat/2488. Загл. с экрана.

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

Microsoft Office профессиональный выпуск версии 2010. Программный пакет «Crypton LITE» («КРИПТОН Шифрование v1.1», «КРИПТОН Подпись v1.1»); Windows 2003 Server; Межсетевой экран; Программный комплекс «КриптоПро АРМ».

7. Материально-техническое обеспечение дисциплины

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 проведе-	Ауд. 332а: Комплекты мебели для учебного процесса. ПЭВМ – 12 (ком-	Ауд.332а: ОС Alt Linux (Альт Образование

ния лабораторных занятий	пьютер Core i5-4570), стенды – 5 шт. Ауд. 424: Комплекты мебели для учебного процесса. ПЭВМ – 12: рабочая станция Регард РДЦБ.; стенды – 3 Ауд. 420: Комплекты мебели для учебного процесса. ПЭВМ-11 (компьютер Core i5-4460), проектор Acer projector X1383WH, экран, стенды – 5 шт., блок управления комплекса радиоконтроля и поиска радиопередающих устройств «ОМЕГА» (переносной), МУ защиты ресурсов сети от внутренних и внешних атак CISCO ASA5505-KB, переносной комплекс для автоматизации измерений при проведении исследований и контроля технических средств ЭВТ «НАВИГАТОР-ПЗГ»; средство активной защиты информации от утечки за счет побочных электромагнитных излучений и наводок «СОНАТА-РЗ.1»; система защиты речевой информации «Соната-АВ-4Б» (Центральный блок питания и управления + Размыкатели в составе СВАЗ Соната АВ); профессиональный обнаружитель скрытых видеокамер СОКОЛ-М (переносной); портативный обнаружитель закладок	8.2) Geany. Lazarus. Qt Creator. Quanta Plus. Вебредактор 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. Ауд.424: ОС Alt Linux (Альт Образование 8.2) Geany. Lazarus. Qt Creator. Quanta Plus. Вебредактор 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. Ауд.420: Microsoft Windows 7 (64 разрядная) Microsoft Office (standart) 2007; Microsoft Access 2007; Microsoft Project 2007; Microsoft Share Point 2007; Microsoft Visio 2007; Microsoft SQL server 2008; 1 С Предприятие Лицензия; 7-Zip File Manager (архиватор); Adobe
	Protect1203 (переносной); устройство активной защиты информации «ВЕТО-М»; электронный замок Samsung SHS-2920	Acrobat Reader; Adobe Flash Player; FAR file manager; Google Chrome; Java TM 7 (64-bit); KLite Codec Pack; Mozilla Firefox; Oracle VM VirtualBox; 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
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 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. 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.

8 Оценочные материалы для промежуточной аттестации обучающихся по дисциплине

8.1 **Оценочные материалы** (ОМ) для дисциплины включают:

перечень компетенций с указанием этапов их формирования в процессе освоения образовательной программы;

описание показателей и критериев оценивания компетенций на различных этапах их формирования, описание шкал оценивания;

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;

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

8.2 Для каждого результата обучения по дисциплине определяются показатели и критерии оценивания сформированности компетенций на различных этапах их формирования, шкалы и процедуры оценивания.

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

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

Документ составлен в соответствии с требованиями ФГОС ВО по специальности 10.05.03 Информационная безопасность автоматизированных систем и специализации Безопасность открытых информационных систем.

ОЦЕНОЧНЫЕ МАТЕРИАЛЫ
ДЛЯ ПРОМЕЖУТОЧНОЙ АТТЕСТАЦИИ

по дисциплине

Криптографические протоколы и стандарты

(наименование дисциплины, практики в соответствии с учебным планом)

1 Перечень компетенций с указанием этапов их формирования

№ п/п	Код компетенции	Содержание компетенции (результат освоения)	В результате изучения учебной дисциплины обучающийся должен:		
			знать	уметь	владеть
1	ПК-14	способностью проводить контрольные проверки работоспособности применяемых программно-аппаратных, криптографических и технических средств защиты информации	типовые криптографические протоколы и основные требования к ним, принципы построения криптографических хеш-функций; протоколы идентификации, протоколы передачи и распределения ключей	использовать симметричные и асимметричные шифросистемы для построения криптографических протоколов, проводить сравнительный анализ криптографических протоколов	навыками систематизации научно-технической информации в сфере криптографической защиты информации

2 Паспорт фонда оценочных средств по дисциплине

№ п/п	Контролируемые модули/разделы/темы дисциплины	Индекс контролируемой компетенции (или ее части)	Оценочные средства	Технология оценки (способ контроля)
1	Понятие криптографического протокола	ПК-14	Экзамен	Контроль преподавателем
			Кейс-задания для практических работ	Проверка преподавателем
			Тестирование	Бланочное тестирование
2	Привязка к биту и электронная жеребьевка	ПК-14	Экзамен	Контроль преподавателем
			Кейс-задания для практических работ	Проверка преподавателем
			Тестирование	Бланочное тестирование
3	Разделение секрета. Прикладные протоколы	ПК-14	Экзамен	Контроль преподавателем
			Кейс-задания для практических работ	Проверка преподавателем
			Доклад	Контроль преподавателем
4	Протоколы идентификации с нулевым разглашением. Протоколы открытых сделок	ПК-14	Экзамен	Контроль преподавателем
			Кейс-задания для практических работ	Проверка преподавателем
			РПР	Проверка преподавателем
5	Построение криптографических хеш-функций. Инфраструктура открытых ключей.	ПК-14	Экзамен	Контроль преподавателем
			Кейс-задания для практических работ	Проверка преподавателем
			РПР	Проверка преподавателем
6	Управление ключами	ПК-14	Экзамен	Контроль преподавателем

			Кейс-задания для практических работ	Проверка преподавателем
			Тестирование	Бланочное тестирование

Оценочные средства для промежуточной аттестации

3.1 Вопросы к собеседованию на экзамене

ПК-14 - способностью проводить контрольные проверки работоспособности применяемых программно-аппаратных, криптографических и технических средств защиты информации

№	Формулировка задания
1	Понятие о криптографических протоколах. Основные виды протоколов. Примитивные и прикладные протоколы.
2	Понятие о криптографических протоколах. Полнота и корректность.
3	Протоколы подбрасывания монеты. Применение протоколов подбрасывания монеты для выработки сеансовых ключей.
4	Связанность и секретность протокола электронной жеребьевки. Пример протокола с безусловной связанностью.
5	Связанность и секретность протокола электронной жеребьевки. Пример протокола с безусловной секретностью.
6	Протоколы привязки к биту. Блоб.
7	Понятие о разделении секрета. Группа доступа, структура доступа. Требования к ним. Минимальная группа доступа.
8	Совершенная СРС (система разделения доступа), идеальная СРС.
9	Пороговые схемы разделения секрета. Схема Шамира, ее совершенность и идеальность.
10	Схема Блэкли. Вопрос о ее совершенности и идеальности.
11	СРС на основе Китайской теоремы об остатках. Вопрос о ее совершенности и идеальности.
12	СРС для произвольной структуры доступа. Вопрос о ее совершенности и идеальности.
13	Протоколы конфиденциальных вычислений.
14	Проверяемое разделение секрета.
15	Протоколы идентификации. Классификация. Требования.
16	Парольные схемы. Разновидности. Область применения.
17	Интерактивные системы доказательств. Полнота, корректность. Пример интерактивной системы доказательств для языка «Квадратичные невычеты».
18	Доказательства с нулевым разглашением. Статистическая неразличимость, вероятностная неразличимость. Пример интерактивного доказательства с нулевым разглашением для языка «Изоморфизм графов».
19	Протоколы идентификации на основе теории ИСД с нулевым разглашением. Схема Фиата-Шамира. Схема Файге-Фиата-Шамира. Их полнота и корректность.
20	Схема идентификации Шнорра. Схема Брикелла-МакКарли. Их полнота и корректность.
21	Схема идентификации Окамото и теорема о ее условной стойкости.
22	Схема Гиллу-Кискатр. Ее полнота и корректность.
23	Слепая подпись.
24	Скрытый канал.
25	Протокол «Покер по телефону».
26	Электронная монета. Электронные деньги. Требования к схемам электронных денег. Схема электронного кошелька с банкнотами одного достоинства.
27	Электронная монета. Электронные деньги. Требования к схемам электронных денег.

	Разного достоинства. Схема с копилкой.
28	Протоколы голосования.
29	Протоколы установления подлинности.
30	Управление ключами. Этапы жизненного цикла ключей. Задачи управления ключами, решаемые криптографическими средствами.
31	Централизованная выработка ключа. Совместная выработка ключа. Требования к секретному ключу. Алгоритм фон Неймана.
32	Распределение ключа при наличии доверенного центра. Распределение секретного ключа без участия доверенного центра.
33	Схемы Wide-Mouth Frog, Yahalom. Их анализ.
34	Протокол Нидхема-Шредера. Его анализ.
35	Протокол Отвея-Рииса. Его анализ.
36	Бесключевой протокол Шамира и атака «Человек посередине».
37	Протокол Диффи-Хэллмана и атака «Человек посередине». Противодействие этой атаке.
38	Протокол Нидхема-Шредера на основе шифра с открытым ключом.
39	Широковещательное распределение ключей.
40	Протокол Kerberos.
41	Инфраструктура открытых ключей. Сертификаты и справочники открытых ключей. Многоуровневая система удостоверяющих центров.

3.2 Кейс-задания для практических работ

ПК-14 - способностью проводить контрольные проверки работоспособности применяемых программно-аппаратных, криптографических и технических средств защиты информации

№ задания	Формулировка вопроса
1.	Используя аффинный мультипликативный алгоритм с ключом P[9] (по модулю 31), зашифровать сообщение “криминал”.
2.	Зашифровать сообщение «пришел увидел победил» при помощи шифра Цезаря y=x+a(mod 31) с криптоключом a=13.
3.	Расшифровать сообщение y, зашифрованное ключом a с помо-щью аддитивного криптопротокола y=x+a(mod 31), a=13, y=эючдущнарчтущнэьпутчщ.
4.	Используя аффинный шифр смещения Цезаря y=x+a(mod n) с параметрами a=P(9), n=31 (P(n) – n-е простое число), расшифровать сообщение y=«щзаьшэшчекэювепдабеычекэювшюкчкшбчпкечгшкучзеэдшцчдючл_дшюк».
5.	Используя аффинный ( ) матричный шифр с ключом «упасть_на_небо», в поле Z31 зашифровать сообщение (в среде Mathcad)«скажи_мне_кто_виноват_и_я_скажу_что_они_с_тобой_сделают».
6.	Используя аффинный мультипликативный алгоритм y=ax(mod n) с ключом a=P(9) (по модулю 31) (P(n) – n-е простое число), расшифровать сообщение y=«пижчрл_лчнхо_уонвфци_нмяцч_жуо_ьощчрл_эхфвли_х_цдхлуз_шлм_бчучэх». В среде Mathcad.
7.	Расшифровать сообщение x, зашифрованное с помощью криптопротокола y=ax+b(mod 31) a=P(8),b=P(7) (P(n) – n-е простое число),y=мсэблжсржтсмжфрпнсумб_дтжижбсодтгсчгиргсмжфрпнстглэгогм.В среде Mathcad.
8.	Распределение ключей в симметричных и асимметричных криптосистемах.
9.	Шифр с самоключом, принцип его реализации.
10.	Симметричные и асимметричные криптосистемы, их определение, основные достоинства и недостатки.
11.	Шифр Виженера, его математическая модель

12.	Примеры шифров замены и перестановки из истории криптографии.
13.	Примеры композиционных шифров.
14.	Перекрытие шифра, его сущность и использование в криптоанализе.
15.	Теоретическая стойкость шифра и ее сущность.
16.	Практическая стойкость шифра и ее сущность.
17.	Характеристики и методы обеспечения имитостойкости. Совершенная имитостойкость.
18.	Основные характеристики псевдослучайных последовательностей
19.	Регистры сдвига с обратной связью. Линейные рекуррентные последовательности.
20.	Линейные регистры сдвига, принципы их построения и использования в криптографии.
21.	Реализация протоколов идентификации на основе симметричных систем шифрования.
22.	Реализация протоколов идентификации на основе асимметричных систем шифрования.
23.	Электронная подпись и принципы ее реализации.
24.	Какова последовательность действий для того, чтобы настроить интерфейсы на маршрутизаторе DioNIS?
25.	Чем режим администратора маршрутизатора DioNIS FW 16000 KB2 отличается от режима оператора?
26.	По нажатию на какую функциональную клавишу открывается карточка интерфейса в криптомаршрутизатореDioNIS FW 16000 KB2?
27.	Используя аффинный ( ) матричный шифр (Y=AX(mod n), n=31) с ключом «дед банзай и его банзайцы», в поле Z31 зашифровать сообщение X=«не откладывайте на завтра то что можно вообще не делать». В среде Mathcad.
28.	Используя аффинный аддитивный алгоритм Аббата Тритемиуса с ключом «плюс», в поле Z31 зашифровать сообщение «правоохранительная деятельность». В среде Mathcad.
29.	Используя аффинный ( ) матричный шифр, зашифровать сообщение Y при помощи матричного криптопротокола . Ключи A и B взять из сообщения "стрельба_глазама".Y="всего_на_всех_не_хватит_потому_что_всего_мало_а_всех_много"
30.	Расшифровать сообщение Y="ьячхьяавчр", зашифрованное с помощью матричного криптопротокола.
31.	Используя аффинный аддитивный алгоритм Аббата Тритемиуса с ключом «роза», в поле Z31 расшифровать сообщение в среде Mathcad."у_одяохбрсщжеохжрглбвчыа_эыпэбзшвэзгбфмпрыимяоиау_оцрыхпфэза".
32.	Проверяемое разделение секрета. Протоколы конфиденциальных вычислений.
33.	Протоколы идентификации на основе ИСД с нулевым разглашением.
34.	Скрытый канал.
35.	Покер по телефону.
36.	Электронная монета. Электронные деньги.
37.	Протоколы голосования.
38.	Управление ключами.
39.	Протокол честной раздачи карт на основе шифра Шамира Карты задаются числовыми значениями начиная с 2 и заканчивая тузом следующим образом: 1. бубны – 101-113; 2. черви – 201-213; 3. кресты – 301-313; 4. пики – 401-413.
40.	Каждый из 5 участников шифрует колоду своим затемняющим множителем, на каждом этапе проверить наличие следующих значений: A B: 364, 6, 68, 518, 151; B C: 313, 28, 486, 377, 17; C D: 66, 111, 318, 483, 500; D E: 216, 180, 32, 441, 564;

	E A: 351, 579, 136, 390, 32.
41.	Схема идентификации Гиллу-Кискате. Данным тестом самопроверки следует пользоваться следующим образом: 1. задать значение параметров p, q, b в протоколе соответствующими; 2. проверить правильность вычисления значения v, подставив параметр u; 3. проверить правильность вычисления значения x, подставив параметр r
42.	проверить правильность вычисления значения y, подставив параметр e; сравнение $x \equiv y^b v^e \pmod{n}$ должно быть верным
43.	задать группу доступа состоящую из всех пяти участников; задать значение секрета m и долей первых 4 участников s_1, s_2, s_3, s_4, в протоколе; в результате правильной работы протокола 5 участник должен получить долю, равную параметру s_5

3.3. РПР

ПК-14 - способностью проводить контрольные проверки работоспособности применяемых программно-аппаратных, криптографических и технических средств защиты информации

№ задания	Формулировка задания
1	Оценить работоспособность схемы обмена секретными ключами. Некто предлагает следующий способ подтверждения того, что вы оба владеете секретным ключом. Вы создаете строку случайных битов, длина которой равна длине ключа, объединяете эту строку случайных битов с ключом при помощи операции XOR и посылаете результат в канал связи. Ваш партнер с помощью операции XOR объединяет полученный блок с ключом (который должен совпадать с вашим) и возвращает результат. Убедившись, что полученная вами строка совпадает с оригинальной, созданной вами, строкой случайных битов, вы заключаете, что ваш партнер имеет тот же секретный ключ, что и вы, хотя ни один из вас не пересылал секретный ключ другому
2	Показать слабость итеративной хэш-функции, основанной на раундовой функции, где Mi -блоки данных, hi-раундовое значение хэш-функции, a и p - известные параметры
3	Разработать для описанной задачи лучший вариант схемы шифрования. Дано: по исходному сообщению вычисляется хэш-функция, объединяется операцией конкатенации с исходным сообщением и результат шифруется по схеме Файстеля, после чего отправляется адресату. Второй вариант: в начале исходное сообщение шифруется по схеме Файстеля, по зашифрованному сообщению вычисляется значение хэш-функции, которое в свою очередь операцией конкатенации присоединяется к зашифрованному сообщению, а результат отсылается адресату
4	Проанализировать алгоритм DES. Если произойдет искажение одного бита символа шифрованного текста при передаче в 8-битовом режиме CFB, на сколько блоков распространится это искажение в полученном сообщении? Имеет ли смысл дважды зашифровывать сообщение с помощью алгоритма DES?
5	Найти значение открытого текста в криптосистеме с открытым ключом, использующей RSA, вы перехватили шифрованный текст C=10, пересылаемый пользователю, открытым ключом которого является e=5, n=35.

3.4. Темы докладов

ПК-14 - способностью проводить контрольные проверки работоспособности применяемых программно-аппаратных, криптографических и технических средств защиты информации

№ задания	Формулировка задания
1.	Построение семейства протоколов KriptoKnight на основе базовых протоколов взаимной аутентификации и распределения ключей

2.	Особенности построения семейства протоколов IPsec.
3.	Протоколы Oakley и особенности их реализации
4.	Протокол ISAKMP и особенности их реализации
5.	Протокол IKE и особенности их реализации
6.	Протоколы SKIP и особенности их реализации
7.	Протоколы SSL/TLS и особенности их реализации
8.	Применение привязки к биту и электронной жеребьевки для совместной выработки ключей.
9.	Применение схем разделения секрета для безопасной отправки сообщений и депонирования ключей.
10.	Идентификация и аутентификация в ОС Windows и Unix.
11.	Разновидности цифровых подписей в электронном документообо-роте.
12.	Схемы электронных денег WebMoney и payCash.
13.	Схемы электронных денег eCash и PayCash.
14.	Криптографические средства в электронном документообороте федеральных и местных органов управления в РФ.
15.	Системы управления криптографическими ключами в федераль-ных и местных органах управления в РФ.
16.	Обзор криптографических протоколов, использующих цифровую подпись.
17.	Практика электронного голосования на примере ЕС.
18.	Применение протокола «Покер по телефону» к раздаче электронных бланков.
19.	Идентификация на основе биометрических данных.

3.5. Тестирование

ПК-14 - способностью проводить контрольные проверки работоспособности применяемых программно-аппаратных, криптографических и технических средств защиты информации

№ задания	Формулировка задания
1.	Семейство обратимых преобразований, каждое из которых определяется некоторым параметром, называемым ключом, а также порядком применения данного преобразования – это: Шифр Шифрсистема Шифртехника Правило зашифрования
2.	Шифры бывают (лишнее исключить): Композиционные Замены Интегральные Перестановки □
3.	Шифры гаммирования бывают (лишнее исключить): Блочные Табличные Модульные □
4.	Криптосистемы RSA и Эль-Гамаля относятся к: Блочным Асимметричным Композиционным Симметричным □
5.	Стойкость асимметричных криптографических систем с открытым ключом основана на: Секретности исходных данных

	Невозможности обратного преобразования однонаправленной функции Секретности алгоритма расшифрования□
6.	В криптографии рассматривают следующие виды стойкости шифров (лишнее исключить): Теоретическая стойкость Вычислительная стойкость Средневзвешенная стойкость□
7.	Шифры перестановки бывают (лишнее исключить): Маршрутные Столбцовые Многозначные □
8.	Методы криптоанализа, использующие статистические характеристики открытых текстов, наиболее эффективны при анализе: Шифров замены Шифров перестановки Шифров гаммирования□
9.	Какую роль играют центры сертификации ключей? Они играют роль доверенной третьей стороны для доказывания факта передачи информации Они служат для регистрации абонентов, изготовления сертификатов открытых ключей, хранения изготовленных сертификатов, поддержания в актуальном состоянии справочника действующих сертификатов и выпуска списка досрочно отозванных сертификатов Они выдают сертификат соответствия длины сгенерированных ключей требованиям нормативных документов
10.	Использование цифровой подписи позволяет не допустить (лишнее исключить): Отказ от авторства Приписывание авторства Несанкционированное ознакомление с подписанным документом
11	Управление секретными ключами включает в себя (лишнее исключить): Пересылку ключей Открытое распределение ключей Схему распределения вычислений Схему разделения секрета □
12	Схемы цифровой подписи бывают (лишнее исключить) Прямыми Обратными Арбитражными
13	Шифры замены бывают (лишнее исключить): Многозначными Однозначными Неоднозначными□
14	Иностранным аналогом стандарта ГОСТ 28147-89 является: Алгоритм А5 Алгоритм DES Алгоритм Гиффорда□
15	Шифр простой замены - это: - шифр, в котором каждый элемент открытого текста преобразуется в соответствующий элемент шифрованного текста с использованием нескольких алфавитов - шифр, в котором ключом шифрования служит достаточно большое простое число - шифр, в котором каждый элемент открытого текста преобразуется в соответствующий элемент шифрованного текста с использованием одного и того же алфавита

16	Шифр перестановки - это: - шифр, в котором при шифровании буквы заменяются некоторыми эквивалентами шифр, в котором при шифровании буквы меняются местами друг с другом в заданном порядке шифр, в котором при шифровании буквы заменяются некоторыми эквивалетнами, после чего меняются друг с другом в заданном порядке
17	К шифрам маршрутной перестановки относятся: шифры гаммирования шифры Сцитала шифры-решетки
18	Шифр Вижинера – это: шифр многоалфавитной замены шифр табличного гаммировния шифр модульного гаммирования
19	Функция Эйлера, используемая в вычислении открытого и закрытого ключей шифрования в алгоритме RSA, вычисляется по формуле: (p-1)*(N-1) (p-1)*(q-1) (N-1)*(q-1)
20	Под энтропией в криптографии понимается: - количество информации на символ передаваемого сообщения - мера неопределенности передаваемого сообщения - количество информации, содержащейся в целом передаваемом сообщении
21	Укажите методы, используемые при криптоанализе блочных шифров: - метод дифференциальных искажений, статистический метод - аналитический метод, метод дифференциальных искажений, статистический метод - аналитический метод, комбинаторный метод, статистический метод
22	В теоретической криптографии исследуются следующие модели шифра (лишнее исключить): алгебраические статические вероятностные
23	Какие данные передаются по незащищенному каналу связи и известны потенциальному злоумышленнику при реализации алгоритма RSA? Криптограмма и открытый ключКриптограмма и закрытый ключ Криптограмма и значение функции Эйлера
24	В чем заключается криптографическая стойкость алгоритма Диффи-Хеллмана? - В проблеме разложения большого числа на простые множители - В проблеме дискретного логарифмирования - В проблеме нахождения наибольшего общего делителя между исходными числами g и p

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 – 2015 Положение о курсовых, экзаменах и зачетах;
- П ВГУИТ 4.1.02 – 2012 Положение о рейтинговой оценке текущей успеваемости.

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

5. Описание показателей и критериев оценивания уровня сформированности компетенций

Результаты обучения по этапам формирования компетенций	Методика оценки (объект, продукт или процесс)	Показатель оценивания	Критерии оценивания сформированности компетенций	Шкала оценивания	
				Академическая оценка или баллы	Уровень освоения компетенции
ПК-14 - способностью проводить контрольные проверки работоспособности применяемых программно-аппаратных, криптографических и технических средств защиты информации					
ЗНАТЬ: типовые криптографические протоколы и основные требования к ним, принципы построения криптографических хеш-функций; протоколы идентификации, протоколы передачи и распределения ключей	Собеседование на экзамене	Уровень знаний	ответил на все вопросы, допустил не более 1 ошибки в ответе	Отлично	Освоена (продвинутый)
			ответил на все вопросы, допустил более 1, но менее 3 ошибок	Хорошо	Освоена (продвинутый)
			ответил не на все вопросы, но в тех, на которые дал ответ не допустил ошибки	Удовлетворительно	Освоена (базовый)
			ответил не на все вопросы, допустил более 5 ошибок	Неудовлетворительно	Не освоена (недостаточный)
УМЕТЬ использовать симметричные и асимметричные шифросистемы для построения криптографических протоколов, проводить сравнительный анализ криптографических протоколов	Кейс-задания для практических работ	Уровень умения	студент выполнил задание и ответил на все вопросы и допустил не более 1 ошибки в ответе	Отлично	Освоена (продвинутый)
			студент выполнил задание и ответил на все вопросы и допустил более 1 ошибки, но менее 3 ошибок	Хорошо	Освоена (продвинутый)
			студент выполнил задание не полностью и ответил не на все вопросы, но в тех, на которые дал ответ не допустил ошибки	Удовлетворительно	Освоена (базовый)
			студент ответил не на все вопросы, допустил более 5 ошибок	Неудовлетворительно	Не освоена (недостаточный)
ВЛАДЕТЬ навыками систематизации научно-технической информации в сфере криптографической защиты информации	Тестирование	Уровень владения материалом	85% и более правильных ответов	Отлично	Освоена (продвинутый)
			75-84% правильных ответов	Хорошо	Освоена (продвинутый)
			65-74% правильных ответов	Удовлетворительно	Освоена (базовый)
			Менее 64% правильных ответов	Не удовлетворительно	Не освоена (недостаточный)
	Доклад	Уровень владения	выставляется студенту при наличии доклада, преобразовании информа-	Зачтено	Освоена (продвинутый, базо-

			ции в единую форму, т.е. презентации по выбранной теме		вый)
			выставляется студенту при наличии информации только из одного источника, и (или) отсутствии презентации по выбранной теме	Не зачтено	Освоена (недостаточный)
	Расчетно-практическая работа	Уровень навыков	студент выбрал верную методику решения задач, ответил на все вопросы, допустил не более 1 ошибки в ответе	Отлично	Освоена (продвинутый)
			студент выбрал верную методику решения задач, проведен верный расчет ответил на все вопросы, имеются незначительные замечания по тексту и оформлению работы, допустил не более 3 ошибок в ответе	Хорошо	Освоена (продвинутый)
			студент выбрал верную методику решения задач, проведен верный расчет, представил решение задач, ответил на все вопросы, имеются значительные замечания по тексту и оформлению работы, допустил не более 5 ошибок в ответе	Удовлетворительно	Освоена (базовый)
			студент выбрал верную методику решения задач, проведен верный расчет, выполнил правильно графическую часть, представил решение задач, ответил на все вопросы, имеются значительные замечания по тексту и оформлению работы, допустил более 5 ошибок в ответе	Не удовлетворительно	Не освоена (недостаточный)