

Минобрнауки России
ФЕДЕРАЛЬНОЕ ГОСУДАРСТВЕННОЕ БЮДЖЕТНОЕ ОБРАЗОВАТЕЛЬНОЕ УЧРЕЖДЕНИЕ
ВЫСШЕГО ОБРАЗОВАНИЯ
«ВОРОНЕЖСКИЙ ГОСУДАРСТВЕННЫЙ УНИВЕРСИТЕТ ИНЖЕНЕРНЫХ ТЕХНОЛОГИЙ»

УТВЕРЖДАЮ
Проректор по учебной работе

(подпись) Василенко В.Н.
(Ф.И.О.)

«25» мая 2023

РАБОЧАЯ ПРОГРАММА ДИСЦИПЛИНЫ

История криптографии

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 освоения дисциплины «История криптографии» являются:

1. реализация информационных технологий в сфере профессиональной деятельности с использованием защищенных автоматизированных систем;
2. управление информационной безопасностью автоматизированных систем.

Поставленная цель достигается решением следующих задач:

1. изучением истории развития криптографии, криптографической терминологии;
2. изучением принципов конструкции и классификации исторических шифров;
3. освоением принципов синтеза и анализа простых криптосистем;
4. освоением понятия криптостойкости и методов, используемых для криптоанализа.

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	ПК-16	способностью участвовать в проведении экспериментально-исследовательских работ при аттестации автоматизированных систем с учетом нормативных документов по защите информации	Историю криптографии	Ориентироваться в истории криптографии, методах защиты и нарушения конфиденциальности информации.	Криптографической терминологией
	ПК-12	способностью участвовать в проектировании системы управления информационной безопасностью автоматизированной системы	Основные государственные стандарты России в области применения криптографических средств	Применять в практической деятельности государственные стандарты России в области применения криптографических средств	Криптографическими средствами защиты информации
	ОК-3	способностью анализировать основные этапы и закономерности исторического развития России, ее место и роль в современном мире для формирования гражданской позиции и развития патриотизма	Основные этапы и закономерности исторического развития России	Применять в практической деятельности основные этапы и закономерности исторического развития России	Современной исторической наукой при организации эксплуатации криптографических средств

3. Место дисциплины в структуре ОП ВО

Дисциплина «История криптографии» относится к блоку 1 ОП и ее вариативной части.

Изучение дисциплины основано на знаниях, умениях и навыках, полученных при изучении обучающимися дисциплины «История».

Дисциплина является предшествующей для изучения дисциплин, прохождения практик:

- Управление информационной безопасностью;
- Организационное и правовое обеспечение информационной безопасности;
- Основы управленческой деятельности;
- Учебная практика, практика по получению первичных профессиональных умений;
- 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 2 зачетных единицы.

Виды учебной работы	Всего часов	Семестр 3
	акад. ч	акад. ч
Общая трудоемкость дисциплины	72	72
Контактная работа, в т.ч. аудиторные занятия:	61,6	61,6
Лекции	30	30
<i>в том числе в форме практической подготовки</i>	–	–
Практические занятия (ПЗ)	30	30
<i>в том числе в форме практической подготовки</i>	30	30
Консультации текущие	1,5	1,5
<i>Виды аттестации – зачет</i>	0,1	0,1
Самостоятельная работа:	10,4	10,4
Аналитический обзор	10,4	10,4

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 раздела дисциплины	Содержание раздела (<i>указываются темы и дидактические единицы</i>)	Трудоемкость раздела, час
1	Криптография в Древнем Мире	Введение в криптографию. Криптография в Древнем мире. Криптография в Средние века.	23
2	Криптография в Новое время	Криптография в эпоху	23
3	Отечественная и современная криптография	Возрождения и Новое время. Криптография в 19 первой половине 20 века. Классификация исторических шифров и их криптоанализ. Криптография во второй половине 20 века и в наше время. Отечественная криптография. Современная криптография.	24,4

5.2 Разделы дисциплины и виды занятий

№ п/п	Наименование раздела дисциплины	Лекции, час	ПЗ (или С), час	СРС, час
1	Криптография в Древнем Мире	10	10	3
2	Криптография время в Новое время	10	10	3
3	Отечественная и современная криптография	10	10	4,4

5.2.1 Лекции

№ п/п	Наименование раздела дисциплины	Тематика лекционных занятий	Трудоемкость, час
1	Криптография в Древнем Мире	Введение в криптографию. Виды криптосистем. Задачи, решаемые методами криптографии. Виды информации, подлежащие закрытию, их модели и свойства. Основные этапы становления криптографии как науки. Специальная терминология.	4
		Криптография в Древнем мире	3
		Криптография в Средние века.	3
2	Криптография в Новое время	Криптография в эпоху Возрождения и Новое время.	4
		Криптография в 19 первой половине 20 века. Механические шифровальные устройства. Дисковые шифраторы. Становление формального подхода.	3
		Классификация исторических шифров и оценка их криптостойкости	3
3	Отечественная и современная криптография	Криптография во II половине 20 века и в наше время. Научный подход.	3
		Отечественная криптография. История развития отечественной криптографии с 16 века до наших дней.	3
		Современная криптография. Криптографические средства в наши дни.	4

5.2.2 Практические занятия (семинары)

№ п/п	Наименование раздела дисциплины	Тематика практических занятий (семинаров)	Трудоемкость, час
1	Криптография в Древнем Мире	Введение в криптографию. Основные понятия криптографии.	4
		Криптография в Древнем мире. Ручное шифрование. Криптоанализ древних шифров.	4
		Криптография в Средние века. Ручное шифрование. Криптоанализ шифров замены методом частотного анализа.	2
2	Криптография в Новое время	Криптография в Новое время. Руч-	4

		ное шифрование и выполнение упражнений по криптоанализу шифров.	
		Криптография в 19 I половине 20 века. Ручное шифрование и выполнение упражнений по криптоанализу шифров.	4
		Классификация исторических шифров и их криптоанализ. Выполнение упражнений на отнесение известных исторических шифров к одному из изученных классов.	2
3	Отечественная и современная криптография	Изучение работ Клода Шеннона.	4
		Изучение работ работ Маркова, Бабаша, Шанкина, Верченко.	4
		Изучение работ работ Диффи, Хэллмана, Шамира, Блюма.	2

5.2.3 Лабораторный практикум не предусмотрен.

5.2.4 Самостоятельная работа обучающихся (СРО)

№ п/п	Наименование раздела дисциплины	Вид СРО	Трудоемкость, час
1	Криптография в Древнем Мире	Аналитический обзор по изучению и анализу криптографических систем в древнем мире	3
2	Криптография в Новое время		3
3	Отечественная и современная криптография		4,4

6 Учебно-методическое и информационное обеспечение дисциплины

6.1 Основная литература

1. Литвинская, О. С. Основы теории передачи информации. Учебное пособие / О.С. Литвинская, Н.И. Чернышев. М.: КноРус, 2015. 168 с.
2. Шнайер, Б. Прикладная криптография. Протоколы, алгоритмы, исходные тексты на языке Си / Б. Шнайер – М.: ТРИУМФ, 2014. – 816 с.

6.2 Дополнительная литература

1. Риксон, Фред Б. Коды, шифры, сигналы и тайная передача информации / Фред Б. Риксон М.: АСТ: Астрель, 2014. – 656 с.
2. Мир математики. Т.2: Жуан Гомес. Математики, шпионы и хакеры. Кодирование и криптография. М.: Де Агостини, 2014. 144 с.

6.3 Перечень учебно-методического обеспечения для самостоятельной работы обучающихся

1. Современная компьютерная безопасность. Теоретические основы. Практические аспекты. Учебное пособие Щербаков А.Ю. Издательство: Книжный мир, 2016 г. <http://www.knigafund.ru/books/88712>
2. Служба защиты информации: организация и управление: учебное пособие для вузов: Аверченков В.И., Рытов М.Ю. Издательство: Флинта, 2017 г. <http://www.knigafund.ru/books/116368>

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 компьютер-	https://niks.su/

ная сеть России	
Информационная система «Единое окно доступа к образовательным ресурсам»	http://window.edu.ru/
Электронная библиотека ВГУИТ	http://biblos.vsu.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.vsu.ru/

6.5 Методические указания для обучающихся по освоению дисциплины

История криптографии [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, В. А. Хвостов; ВГУИТ, Кафедра информационной безопасности. Воронеж : ВГУИТ, 2016. – 13 с. <<http://biblos.vsu.ru/MegaPro>>

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

Microsoft Windows 7 (64 разрядная) Профессиональная Лицензия (DreamSpark); Microsoft Office (standart) 2007 Профессиональная Лицензия (DreamSpark); Microsoft Access 2007 Профессиональная Лицензия (DreamSpark); Microsoft Project 2007 Профессиональная Лицензия (DreamSpark); Microsoft Share Point 2007.

Профессиональная Лицензия (DreamSpark); Microsoft Visio 2007 Профессиональная Лицензия (DreamSpark) Microsoft SQL server 2008 Профессиональная Лицензия (DreamSpark); 1 С Предприятие Лицензия; 7-Zip File Manager (архиватор) Бесплатное ПО; Adobe Acrobat Reader Бесплатное ПО; Adobe Flash Player Бесплатное ПО; FAR file manager Бесплатное ПО; Google Chrome Бесплатное ПО; Java TM 7 (64-bit) Бесплатное ПО; K-Lite Codec Pack Бесплатное ПО; Mozilla Firefox Бесплатное ПО; Oracle VM VirtualBox Бесплатное ПО; Sublime Text Бесплатное ПО; Symantec Endpoint Protection 12 (Заменен на AVP Kaspersky) Бесплатное ПО; VMWare Player Бесплатное ПО; Антивирус “Зоркий глаз” Бесплатное ПО; Lazarus (аналог Delphi) Бесплатное ПО; SmathStudio (аналог Mathcad) Бесплатное ПО; NanoCAD (аналог Autocad) Бесплатное ПО; Gimp (графический редактор аналог Photoshop) Бесплатное ПО; Avidemax (видео редактор) Бесплатное ПО; Virtual Dub (видео редактор) Бесплатное ПО; Free Pascal Бесплатное ПО; 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

7 Материально-техническое обеспечение дисциплины

Комплекты мебели для учебного процесса.

ПЭВМ-12 (компьютер Core i5-4460), проектор Acer projector X1383WH, 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 «СонатаАВ-4Б» (Центральный блок питания и управления + Размыкатели в составе СВАЗ Соната АВ); профессиональный обнаружитель скрытых видеокамер СОКОЛ-М (переносной); портативный обнаружитель закладок Protect1203 (переносной); устройство активной защиты информации «ВЕТО-М»; электронный замок Samsung SHS-2920.

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 СРЕДСТВА
ДЛЯ ПРОМЕЖУТОЧНОЙ АТТЕСТАЦИИ**

по дисциплине/практике

История криптографии

1 Перечень компетенций с указанием этапов их формирования

№ п/п	Перечень компетенций		Этапы формирования компетенций		
	Код компетенции	Содержание компетенции (результат освоения)	В результате изучения учебной дисциплины обучающийся должен:		
			знать	уметь	владеть
1	ПК-16	способностью участвовать в проведении экспериментальных исследований работ при аттестации автоматизированных систем с учетом нормативных документов по защите информации	Историю криптографии.	Ориентироваться в истории криптографии, методах защиты и нарушения конфиденциальности информации.	Криптографической терминологией
2	ПК-12	способностью участвовать в проектировании системы управления информационно-й безопасностью автоматизированной системы	Основные государственные стандарты России в области применения криптографических средств	Применять в практической деятельности государственные стандарты России в области применения криптографических средств	Криптографическими средствами защиты информации
3	ОК-3	способностью анализировать основные этапы и закономерности исторического развития России, ее место и роль в современном мире для формирования гражданской позиции и развития патриотизма	Основные этапы и закономерности исторического развития России	Применять в практической деятельности основные этапы и закономерности исторического развития России	Современной исторической наукой при организации эксплуатации криптографических средств

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 2	Криптография в Древнем Мире Криптография в Новое время Отечественная и современная криптография	ПК-16 ПК-12 ОК-3	Зачет	№1-30	Отметка «зачтено- не зачтено»
			Контрольные вопросы к текущим опросам на практических работах	№31-47	Уровневая шкала
			Задания к практическим работам	№ 31-47	Уровневая шкала
			Доклад	№ 48	Уровневая шкала

3 Оценочные средства для промежуточной аттестации.

Вопросы к зачету

3.1.1. Шифр и наименование компетенции ПК-16 - Способность участвовать в проведении экспериментально-исследовательских работ при аттестации автоматизированных систем с учетом нормативных документов по защите информации ПК-12 способностью участвовать в проектировании системы управления информационной безопасностью автоматизированной системы ОК-3 способностью анализировать основные этапы и закономерности исторического развития России, ее место и роль в современном мире для формирования гражданской позиции и развития патриотизма

1	Введение в криптографию. Основные понятия и определения. Виды криптосистем. Задачи, решаемые методами криптографии.
2	Виды информации, подлежащие закрытию, их модели и свойства.
3	Основные этапы становления криптографии как науки.
4	Специальная терминология в криптографии.
5	Криптография в Древнем Египте и Месопотамии. Кодирование и скрытие информации. Понятие о стеганографии.
6	Криптография в Древней Греции и Древнем Риме. Простейшие шифры перестановки и замены. Сциталла. Шифр Цезаря. Шифр Полибия. Шифр Энея.
7	Криптография в средневековой Европе. Каббала и шифр атбаш. Криптография в арабском мире — шифр дауди, Абу Бакр Ахмед бен-Али бен-Вахшиян-Набат, ШехабКалкашанди, зарождение частотного анализа.
8	Криптография в Новое время. Криптография в эпоху Возрождения и Новое 19 время. Церковные шифры. Лозунговый шифр. Шифры Тритемиуса, Виженера. Номенклаторы.
9	Возникновение государственных криптографических служб в 16-17 вв.
10	Шифр Наполеона.
11	Работы Джеймса Ловелла. Становление американской криптографии.
12	Тест Казиски. Принцип Керкгоффа. Становление формального подхода. Криптография в годы I мировой войны. Шифр Вернама.
13	Русская криптография в допетровское время. Развитие криптографических служб при Петре I. Цифирь Петра I.
14	Становление криптографических служб в Советской России и СССР. Спецотдел по криптографии при ВЧК. Первые советские шифровальные и кодировочные машины.
15	Механические шифровальные устройства. Дисковые шифраторы.
16	Шифр Хейглина. Криптография в годы II мировой войны. Епигма и ее вскрытие. Вклад Чарльза Бэббиджа и Алана Тьюринга в криптографию.
17	Работы Э. Шелдона, Н. Винера и К. Шеннона как научная основа современной криптографии и теории информации.
18	Информационное противоборство в годы Революции и Гражданской войны в России.
19	Информационное противоборство в годы ВОВ и Холодной войны. Создание и работа Высшей школы криптографов.
20	Выдающиеся современные криптографы и их вклад в развитие науки. Отечественные и международные премии и награды в области криптологии.
21	Классификация исторических шифров и их криптоанализ. Шифры замены, перестановки, гаммирования. Композиции шифров. Способы их вскрытия. Частотный анализ и атака по словарю. Тест Казиски. Вскрытие одноразового блокнота (операция Venona).
22	Первые компьютерные шифры. Понятие о блочных шифрах. Первый блочный шифр — Lucifer.
23	Понятие о поточных шифрах. Военные поточные шифры в годы Холодной войны.

24	Работы У. Диффи, М.Хэллмана и Р. Меркла — основоположников криптографии с открытым ключом. Понятие о шифре с открытым ключом и цифровой подписи.
25	Развитие гражданской криптографии в СССР и России.
26	Криптографические средства в наши дни. Задачи, решаемые современной криптографией. Математический аппарат, используемый современной криптологией.
27	Обеспечение безопасности связи.
28	Электронные платежи.
29	Криптографические протоколы в компьютерных сетях.
30	Задачи аутентификации.

3.2

Задания к практическим работам

3.2.1 Шифр и наименование компетенции ПК-16 - Способность участвовать в проведении экспериментально-исследовательских работ при аттестации автоматизированных систем с учетом нормативных документов по защите информации ПК-12 способностью участвовать в проектировании системы управления информационной безопасностью автоматизированной системы ОК-3 способностью анализировать основные этапы и закономерности исторического развития России, ее место и роль в современном мире для формирования гражданской позиции и развития патриотизма

№ задания	Условие задачи (формулировка задания)
31	Зашифровать свою фамилию с помощью шифра атбаш.
32	Дешифровать сообщение, зашифрованное с помощью шифра атбаш.
33	Зашифровать свою фамилию с помощью шифра Цезаря.
34	Дешифровать сообщение, зашифрованное шифром Цезаря.
35	Зашифровать свою фамилию с помощью квадрата Полибия 6x6
36	Дешифровать сообщение, зашифрованное с помощью квадрата Полибия 6x6
37	Зашифровать свою фамилию с помощью таблицы Виженера. В качестве ключа использовать свое имя.
38	Дешифровать сообщение, зашифрованное с помощью таблицы Виженера.
39	Дешифровать сообщение, зашифрованное с помощью прямоугольника Плейфейра.
40	Зашифровать сообщение «Hide the gold in the tree stump». Ключ «playfairexample»
41	Расшифровать послание Шерлока Холмса.
42	Придумать свой шифр из цифр.
43	Придумать свой шифр из букв русского алфавита.
44	Придумать свой шифр из букв алфавита английского языка.
45	Оценить стойкость к подбору придуманный шифр из цифр.
46	Оценить стойкость к подбору придуманный шифр из букв русского алфавита.
47	Оценить стойкость к подбору придуманный шифр из букв алфавита английского языка.

3.3 Темы докладов и презентаций

Шифр и наименование компетенции ПК-16 - Способность участвовать в проведении экспериментально-исследовательских работ при аттестации автоматизированных систем с учетом нормативных документов по защите информации ПК-12 способностью участвовать в проектировании системы управления информационной безопасностью автоматизированной системы ОК-3 способностью анализировать основные этапы и закономерности исторического развития России, ее место и роль в современном мире для формирования гражданской позиции и развития патриотизма

№ задания	Тема доклада
48	«Криптография в древнем мире»

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, а также методическими указаниями ...*(перечислить если имеются в наличии)*.

В методических указаниях указывается порядок проведения оценки знаний, умений, навыков и (или) опыта деятельности, характеризующих этапы формирования компетенций, и выставления оценки по дисциплине (средневзвешенная – среднеарифметическое из всех оценок в течение периода изучения дисциплины; с использованием штрафных баллов за недочеты; интегральная – суммирование набранных баллов за каждое задание и пр.) **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 ПК-16 -способность участвовать в проведении экспериментально-исследовательских работ при аттестации автоматизированных систем с учетом нормативных документов по защите информации.					
ЗНАТЬ: Основные понятия и методы обеспечения информационной безопасности, применяемые в зарубежных стандартах.	Зачет	Уровень владения материалом	ответил не на все вопросы, допустил более 5 ошибок	Не зачтено	Не освоена (недостаточный)
			ответил на все вопросы, допустил не более 1 ошибки в ответе	Зачтено	Освоена (базовый, повышенный)
УМЕТЬ: Пользоваться расчетными соотношениями и используемыми в зарубежных стандартах в области информационной безопасности.	Контрольные вопросы к текущим опросам по практическим работам	Уровень умения	выполнил задание и ответил на все вопросы и допустил не более 1 ошибки в ответе	Отлично	Освоена
			выполнил задание и ответил на все вопросы и допустил более 1 ошибки, но менее 3 ошибок	Хорошо	Освоена
			выполнил задание не полностью и ответил не на все вопросы, но в тех, на которые дал ответ не допустил ошибки	Удовлетворительно	Освоена
			ответил не на все вопросы, допустил более 5 ошибок	Неудовлетворительно	Не освоена
	Задания к практическим работам	Уровень умения	выполнил задание и ответил на все вопросы и допустил не более 1 ошибки в ответе	Отлично	Освоена
		выполнил задание и ответил на все	Хорошо	Освоена	

			вопросы и допустил более 1 ошибки, но менее 3 ошибок		
			выполнил задание не полностью и ответил не на все вопросы, но в тех, на которые дал ответ не допустил ошибки	Удовлетворительно	Освоена
			ответил не на все вопросы, допустил более 5 ошибок	Неудовлетворительно	Не освоена
ВЛАДЕТЬ: Навыками применения математического аппарата для решения прикладных задач обеспечения информационной безопасности, используемых в зарубежных стандартах.	Доклад	Уровень владения	выставляется обучающемуся при наличии доклада, преобразовании информации в единую форму, т.е. презентации по выбранной теме	Зачтено	Освоена
			выставляется обучающемуся при наличии информации только из одного источника, и (или) отсутствии презентации по выбранной теме	Не зачтено	Не освоена