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

УТВЕРЖДАЮ
Проректор по учебной работе

ДОКУМЕНТ ПОДПИСАН
ЭЛЕКТРОННОЙ ПОДПИСЬЮ

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

_____ _Василенко В.Н._
(подпись) (Ф.И.О.)

«26» мая 2022

РАБОЧАЯ ПРОГРАММА ДИСЦИПЛИНЫ

История криптографии

Специальность

10.05.03 Информационная безопасность автоматизированных систем

Специализация

Безопасность открытых информационных систем

Квалификация (степень) выпускника

специалист по защите информации

Разработчик _____ _____ _____
(подпись) (дата) (Ф.И.О.)

СОГЛАСОВАНО:

Заведующий кафедрой _____информационной безопасности_____
(наименование кафедры, являющейся ответственной за данное направление подготовки, профиль)

_____ _____ _____Скрыпников А.В._____
(подпись) (дата) (Ф.И.О.)

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	Криптографическим и 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
в том числе в форме практической подготовки	–	–
Практические занятия (ПЗ)	30	30
в том числе в форме практической подготовки	–	–
Консультации текущие	1,5	1,5
Виды аттестации – зачет	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	енование раздела дисциплины	Содержание раздела *(указываются темы и дидактические единицы)*	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 работДиффи, 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 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

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.vsuet.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 ReaderБесплатное ПО; Adobe Flash Player Бесплатное ПО; FAR file managerБесплатное ПО; Google ChromeБесплатное ПО; Java TM 7 (64-bit)Бесплатное ПО; K-Lite Codec PackБесплатное ПО; Mozilla FirefoxБесплатное ПО; Oracle VM VirtualBoxБесплатное ПО; Sublime TextБесплатное ПО; Symantec Endpoint Protection 12 (Заменен на AVP Kaspersky)Бесплатное ПО; VMWare PlayerБесплатное ПО; Антивирус “Зоркий глаз”Бесплатное ПО; Lazarus (аналог Delphi)Бесплатное ПО; SmathStudio (аналог Mathcad) Бесплатное ПО; NanoCAD (аналог Autocad) Бесплатное ПО; Gimp (графичский 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 про-

ведении исследований и контроля технических средств ЭВТ «НАВИГАТОР-ПЗГ»; средство активной защиты информации от утечки за счет побочных электромагнитных излучений и наводок «СОНАТА-Р3.1»; 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 замо5к 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.

АННОТАЦИЯ
К РАБОЧЕЙ ПРОГРАММЕ
ДИСЦИПЛИНЫ
«ИСТОРИЯ КРИПТОГРАФИИ»
(наименование дисциплины)

Процесс изучения дисциплины направлен на формирование следующих компетенций:

– способностью применять языки, системы и инструментальные средства программирования в профессиональной деятельности (ОПК-3);

– способностью участвовать в проектировании системы управления информационной безопасностью автоматизированной системы (ПК-12);

–способностью участвовать в проведении экспериментально-исследовательских работ при аттестации автоматизированных систем с учетом нормативных документов по защите информации (ПК-16).

В результате освоения дисциплины обучающийся должен:

Знать

– Историю криптографии. Основы оценки и анализа систем шифрования используемые на ранних стадиях развития теории шифрования. Современные методы криптопреобразования информации и криптоанализа.

Уметь

– Ориентироваться в истории криптографии, методах защиты и нарушения конфиденциальности информации. Осуществлять применение и оценку криптостойкости шифров, применяемых на ранних стадиях развития теории шифрования. Осуществлять сбор, обработку, анализ и систематизацию научно-технической информации в области теории шифрования.

Владеть

–Криптографической терминологией. Навыками анализа методов шифрования. Навыками анализа криптостойкости различных систем шифрования. Навыками проектирования криптосистем.

Содержание разделов дисциплины. Введение в криптографию. Криптография в Древнем мире. Криптография в Средние века. Криптография в эпоху 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.