МИНИСТЕРСТВО ВЫСШЕГО ОБРАЗОВАНИЯ И НАУКИ
РОССИЙСКОЙ ФЕДЕРАЦИИ
ФЕДЕРАЛЬНОЕ ГОСУДАРСТВЕННОЕ БЮДЖЕТНОЕ ОБРАЗОВАТЕЛЬНОЕ
УЧРЕЖДЕНИЕ ВЫСШЕГО ОБРАЗОВАНИЯ
«БЕЛГОРОДСКИЙ ГОСУДАРСТВЕННЫЙ
ТЕХНОЛОГИЧЕСКИЙ УНИВЕРСИТЕТ им. В.Г.ШУХОВА»
Северо-Кавказский филиал

УТВЕРЖДАЮ:
Директор СКФ БГТУ
им. В.Г. Шухова
_____В.Л. Курбатов
«24» февраля 2021 г.

РАБОЧАЯ ПРОГРАММА УЧЕБНОЙ ДИСЦИПЛИНЫ

ЕН.03 Основы криптографии

Специальность

10.02.05 Обеспечение информационной безопасности автоматизированных систем

Квалификация выпускника

Техник по защите информации

Форма обучения

очная

Срок обучения

3 года 10 месяцев

Минеральные Воды, 2021 г.

Рабочая программа составлена на основании требований:

- Федерального государственного образовательного стандарта среднего профессионального образования (далее ФГОС СПО) по специальности 10.02.05 «Обеспечение информационной безопасности автоматизированных систем», утвержденного Приказом Министерства образования и науки РФ № 1553 от 09.12.2016 г.,
- Плана учебного процесса БГТУ им. В.Г. Шухова по специальности 10.02.05 «Обеспечение информационной безопасности автоматизированных систем», утвержденного в 2021 г.

Организация разработчик: СКФ ФГБОУ ВО «БГТУ им. В.Г. Шухова», Северо-Кавказский филиал

Составитель: к.пед.н.  И.В. Черкасова

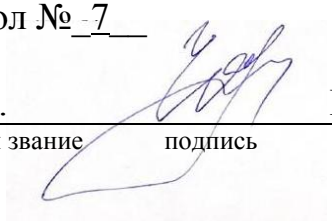
ученая степень и звание подпись инициалы, фамилия

Рабочая программа обсуждена и рекомендована на заседании кафедры

Экономических и естественно-научных дисциплин

название кафедры

«_24_» _февраля_ 2021 г., протокол № _7__

Заведующий кафедрой: к.пед.н.  И.В. Черкасова

ученая степень и звание подпись инициалы, фамилия

СОДЕРЖАНИЕ

1. ОБЩАЯ ХАРАКТЕРИСТИКА РАБОЧЕЙ ПРОГРАММЫ УЧЕБНОЙ ДИСЦИПЛИНЫ

«ЕН.03. Основы криптографии»

1.1. Область применения программы

Рабочая программа учебной дисциплины является частью основной образовательной программы в соответствии с ФГОС СПО 10.02.05 «Обеспечение информационной безопасности автоматизированных систем» (квалификация «Техник по защите информации»).

1.2. Цель и планируемые результаты освоения дисциплины:

Целью освоения дисциплины является формирование у обучающихся знаний, умений, навыков и опыта деятельности, характеризующих этапы формирования компетенций и обеспечивающих достижение планируемых результатов освоения образовательной программы, а также ознакомление с математическими методами современной криптографии и применением их к задаче защиты информации.

В результате освоения учебной дисциплины обучающийся должен:

уметь:

- конструировать криптостойкие алгоритмы и протоколы;
- проводить анализ криптостойкости алгоритмов и протоколов;
- создавать программы, реализующие алгоритмы и протоколы защищенной передачи данных;

знать:

- основные направления развития криптографии, теории информации и теории кодирования;
- основные принципы построения кодов, криптосистем и крипто протоколов;
- основные методы анализа криптостойкости информационных систем;
- основные алгоритмы шифрования;
- основные протоколы защищенной передачи данных.

1.3. Место дисциплины в структуре основной профессиональной образовательной программы:

Учебная дисциплина «Основы криптографии» относится к дисциплинам математического и общего естественнонаучного учебного цикла общеобразовательной программы «Обеспечение информационной безопасности автоматизированных систем». Для освоения дисциплины необходимы полученные знания и умения по дисциплине «Информатика». Освоение данной дисциплины является необходимым условием для последующего изучения дисциплин: «Обеспечение комплексной безопасности объектов информатизации», «Организационная защита информации», «Программные и программно-аппаратные средства обеспечения информационной безопасности», «Криптографические средства и методы защиты информации». Изучается обучающимися очной формы обучения в **3** семестре.

1.4. Планируемые результаты освоения учебной дисциплины

В результате изучения учебной дисциплины обучающийся должен освоить соответствующие компетенции:

Код	Общие компетенции
ОК 01	Выбирать способы решения задач профессиональной деятельности, применительно к различным контекстам

ОК 02	Осуществлять поиск, анализ и интерпретацию информации, необходимой для выполнения задач профессиональной деятельности
ОК 03	Планировать и реализовывать собственное профессиональное и личностное развитие
ПК 2.4	Осуществлять обработку, хранение и передачу информации ограниченного доступа

В результате освоения учебной дисциплины обучающийся должен:

уметь	Распознавать задачу и/или проблему в профессиональном и/или социальном контексте; анализировать задачу и/или проблему и выделять её составные части; определять этапы решения задачи; выявлять и эффективно искать информацию, необходимую для решения задачи и/или проблемы; составить план действия; определить необходимые ресурсы; владеть актуальными методами работы в профессиональной и смежных сферах; реализовать составленный план; оценивать результат и последствия своих действий (самостоятельно или с помощью наставника). Определять задачи поиска информации; определять необходимые источники информации; планировать процесс поиска; структурировать получаемую информацию; выделять наиболее значимое в перечне информации; оценивать практическую значимость результатов поиска; оформлять результаты поиска. Определять актуальность нормативно-правовой документации в профессиональной деятельности; выстраивать траектории профессионального и личностного развития. Применять программные и программно-аппаратные средства для защиты информации в базах данных; проверять выполнение требований по защите информации от несанкционированного доступа при аттестации объектов информатизации по требованиям безопасности информации; применять математический аппарат для выполнения криптографических преобразований; использовать типовые программные криптографические средства, в том числе электронную подпись.
знать	Актуальный профессиональный и социальный контекст, в котором приходится работать и жить; основные источники информации и ресурсы для решения задач и проблем в профессиональном и/или социальном контексте. алгоритмы выполнения работ в профессиональной и смежных областях; методы работы в профессиональной и смежных сферах; структуру плана для решения задач; порядок оценки результатов решения задач профессиональной деятельности. Номенклатура информационных источников применяемых в профессиональной деятельности; приемы структурирования информации; формат оформления результатов поиска информации. Содержание актуальной нормативно-правовой документации; современная научная и профессиональная терминология; возможные траектории профессионального развития и самообразования. Особенности и способы применения программных и программно-аппаратных средств защиты информации, в том числе, в операционных системах, компьютерных сетях, базах данных; типовые модели управления доступом, средств, методов и протоколов идентификации и аутентификации; основные понятия криптографии и типовых криптографических методов и средств защиты информации.
Иметь практический	Решение задач защиты от НСД к информации ограниченного доступа с

опыт	помощью программных и программно-аппаратных средств защиты информации; применение электронной подписи, симметричных и асимметричных криптографических алгоритмов и средств шифрования данных.

1.5. Общее количество часов на освоение программы учебной дисциплины: всего –50 часов, в том числе:

максимальной учебной нагрузки обучающегося **– 50 часов**, включая:

обязательной аудиторной учебной нагрузки обучающегося – 48 часов;

самостоятельной работы обучающегося – 2 часа.

По итогам обучения ЕН.03. «Основы криптографии» предусмотрен дифференцированный зачет **в 3 семестре**.

2. СТРУКТУРА И СОДЕРЖАНИЕ УЧЕБНОЙ ДИСЦИПЛИНЫ

2.1. Объем учебной дисциплины и виды учебной работы

Вид учебной работы	Объем часов
Максимальная учебная нагрузка (всего)	50
Обязательная аудиторная учебная нагрузка(всего)	48
в том числе:	
лекции	32
практические занятия	16
лабораторные	-
Самостоятельная работа обучающегося(всего)	2
Форма промежуточной аттестации обучающегося (диф. зачет/зачет/ экзамен), семестр	Диф.зачет – 3 семестр

2.2. Тематический план и содержание учебной дисциплины

Наименование разделов учебной дисциплины	Содержание учебного материала, лабораторных работ и практических занятий, внеаудиторной (самостоятельной) учебной работы обучающихся, курсового (работы) проекта *(если предусмотрены)*		Объем часов	Уровень усвоения
1	2		3	4
ЕН.03 Основы криптографии			**50**	
Раздел 1. Основы и содержание криптографии	1	**Содержание учебного материала**	**24**	
	1.1	Лекция №1 Основные понятия криптографии	4	ознакомитель-ный
	1.2	Лекция №2 Основные классы шифров и их свойства	4	ознакомитель-ный
	1.3	Лекция №3 Надёжность шифров	4	репродуктивный
	1.4	Лекция №4 Случайные числа в криптографии	4	репродуктивный
	2	**В том числе, практических занятий**	**8**	
	2.1	Практическое занятие №1 Основные этапы становления криптографии как науки. Частотные характеристики открытых текстов. k-граммная модель открытого текста. Критерии распознавания открытого текста	2	репродуктивный
	2.2	Практическое занятие №2 Разновидности шифров перестановки: маршрутные и геометрические перестановки. Поточные шифры замены Шифры гаммирования и их анализ. Использование неравновероятной гаммы, повторное использование гаммы, криптоанализ шифра Виженера. Тесты У.Фридмана. Блочные шифры замены. Современные блочные шифры.	2	репродуктивный
	2.3	Практическое занятие №3 Основы теории К.Шеннона. Криптографическая стойкость шифров. Теоретически стойкие шифры. Шифры, совершенные при нападении на открытый текст. Шифры, совершенные при нападении на ключ. Практически стойкие шифры. Вопросы имитозащиты. Имитостойкость шифров. Характеристики имитостойкости шифров и их оценки. Примеры имитостойких и неимитостойких шифров. Методы имитозащиты неимитостойких шифров. Помехоустойчивость шифров. Шифры, не размножающие	2	репродуктивный

		искажений типа замены знаков. Шифры, не размножающие искажений типа пропуск-вставка знаков.		
	2.4	Практическое занятие №4 Физические генераторы случайных чисел. Генераторы псевдослучайных чисел: конгруэнтные генераторы, сдвиговые регистры, сдвиговый регистр с линейной обратной связью, сдвиговые регистры с нелинейной обратной связью.	2	репродуктивный
Раздел 2. Криптосистемы и их характеристика		**Содержание учебного материала**	**24**	
	1.1	Лекция №5 Симметричные криптосистемы	4	ознакомитель-ный
	1.2	Лекция №6 Асимметричные криптосистемы	4	ознакомитель-ный
	1.3	Лекция №7 Методы синтеза и анализа криптосистем	4	репродуктивный
	1.4	Лекция №8 Криптографические алгоритмы и протоколы	4	
	2	**В том числе, практических занятий**	**8**	
	2.1	Практическое занятие №5 Системы шифрования Виженера. Псевдослучайные генераторы. Гаммирование. Стандарты шифрования DES и ГОСТ. Моноалфавитные и многоалфавитные подстановки. Системы шифрования Виженера. Псевдослучайные генераторы.	2	репродуктивный
	2.2	Практическое занятие №6 Алгоритм RSA. Криптографические хэш функции. Криптосистемы на эллиптических ключах. Изучение ассиметричных криптосистем, процедур аутентификации и ЭЦП. Криптосистемы без передачи ключей. Алгоритм Эль-Гамаля.	2	репродуктивный
	2.3	Практическое занятие №7 Разработка и реализация варианта симметричного криптографического алгоритма с AES – подобной структурой. Асимметричные системы шифрования: схема ДиффиХеллмана, схема Эль-Гамаля. Схема RSA: алгоритм шифрования.	2	репродуктивный
	2.4	Практическое занятие №8 Распределение ключей. Методы экспоненциального ключевого обмена. Цифровая (электронная) подпись, протоколы аутентификации. Протоколы удаленной аутентификации.	2	репродуктивный
Самостоятельная работа обучающихся			**2**	

Тематика внеаудиторной самостоятельной работы (написание эссе на темы): 1 Классификация атак на криптоалгоритм. 2 Модель злоумышленника, классификация злоумышленников. 3 Некриптографические методы защиты информации.	**2**	продуктивный
Промежуточная аттестация	**-**	
Всего:	**50**	

3. УСЛОВИЯ РЕАЛИЗАЦИИ ПРОГРАММЫ УЧЕБНОЙ ДИСЦИПЛИНЫ

3.1. Наименование учебных помещений и помещений для самостоятельной работы

Наименование учебных помещений* и помещений для самостоятельной работы	Оснащенность учебных помещений и помещений для самостоятельной работы	Перечень лицензионного и свободно распространяемого программного обеспечения. Реквизиты подтверждающего документа
Кабинет информатики. № 20. для проведения лекций Кабинет информатики. № 20. для проведения практических занятий Кабинет информатики. № 20. для проведения групповых и индивидуальных консультаций Кабинет информатики. № 20. для текущего контроля и промежуточной аттестации	Лаборатория технических средств защиты информации. Оснащен информационными стендами, по 10 компьютеров на базе процессора DualCore Intel Core i3, оперативной памятью 4ГБ и жестким диском 500 ГБ, локальной сетью с пропускной способностью 100 Мбит/с, операционная система Windows 7 (32-bit) учебной доской, учебно-методическими пособиями, наглядными пособиями, стульями на 1 ученика 1 стул, столами 1 шт. на 2 человек, Оснащена аппаратными средствами аутентификации пользователя; средствами защиты информации от утечки по акустическому (виброаккустическому) каналу и каналу побочных электромагнитных излучений и наводок; средствами измерения параметров физических полей (электромагнитных излучений и наводок, акустических (виброакустических) колебаний и т.д.); стендами физической защиты объектов информатизации, оснащенными средствами контроля доступа, системами видеонаблюдения и охраны объектов	1. Операционная системаWindows 7 (License № 64080343 от 15.09.2014); 2.Офисный пакет приложений MicrosoftOffice 2007 (License№43846774 от 25.02.2008)

3.2. Информационное обеспечение обучения: перечень рекомендуемых учебных изданий, интернет-ресурсов, дополнительной литературы, периодических изданий, программного обеспечения

3.2.1 Основная литература

1. Коржик, В. И. Основы криптографии : учебное пособие / В. И. Коржик, В. А. Яковлев. — Санкт-Петербург : Интермедия, 2017. — 312 с. — ISBN 978-5-89160-097-3. — Текст : электронный // Электронно-библиотечная система IPR BOOKS : [сайт]. — URL: http://www.iprbookshop.ru/66798.html. — Режим доступа: для авторизир. пользователей

2. Басалова, Г. В. Основы криптографии : учебное пособие / Г. В. Басалова. — 3-е изд. — Москва, Саратов : Интернет-Университет Информационных Технологий (ИНТУИТ), Ай Пи Ар Медиа, 2020. — 282 с — ISBN 978-5-4497-0340-8. — Текст : электронный // Электронно-библиотечная система IPR BOOKS : [сайт]. — URL: https://www.iprbookshop.ru/89455.html. — Режим доступа: для авторизир. пользователей

3.2.2 Дополнительная литература:

1. Баричев С.Г, Серов Р.Е. Основы современной криптографии. -Москва : М.: Горячая линия - Телеком, 2002 http://window.edu.ru/resource/005/24005

2. Калинкина Т.И., Ильин М.Е., Пржегорлинский В.Н. Криптографическая защита информации в объектах информационной инфраструктуры: учебник для СПО / Т.И.

Калинкина, М.Е. Ильин, В.Н. Пржегорлинский. – Москва: Академия, 2020. – 288 с. – ISBN 978-5-4468-8717-0 https://academia-library.ru/catalogue/4893/444518/

3. Фороузан, Б. А. Криптография и безопасность сетей : учебное пособие / Б. А. Фороузан ; под редакцией А. Н. Берлина. — 3-е изд. — Москва : Интернет-Университет Информационных Технологий (ИНТУИТ), Ай Пи Ар Медиа, 2021. — 776 c. — ISBN 978-5-4497-0946-2. — Текст : электронный // Электронно-библиотечная система IPR BOOKS : [сайт]. — URL: http://www.iprbookshop.ru/102017.html

4. Мэйволд, Э. Безопасность сетей : учебное пособие / Э. Мэйволд. — 3-е изд. — Москва : Интернет-Университет Информационных Технологий (ИНТУИТ), Ай Пи Ар Медиа, 2021. — 571 c. — ISBN 978-5-4497-0863-2. — Текст : электронный // Электронно-библиотечная система IPR BOOKS : [сайт]. — URL: http://www.iprbookshop.ru/101992.html

5. Криптография и безопасность цифровых систем : учебное пособие / В. Г. Грибунин, А. П. Мартынов, Д. Б. Николаев, В. Н. Фомченко ; под редакцией А. И. Астайкин. — Саров : Российский федеральный ядерный центр – ВНИИЭФ, 2011. — 411 c. — ISBN 978-5-9515-0166-0. — Текст : электронный // Электронно-библиотечная система IPR BOOKS : [сайт]. — URL: http://www.iprbookshop.ru/60851.html

3.2.3 Официальные, справочно-библиографические и периодические издания

1. Конституция Российской Федерации : принята всенар. голосованием 12 дек. 1993 г. [с учетом поправок, внесенных Законами Рос. Федерации о поправках к Конституции Рос. Федерации от 30 дек. 2008 г. № 6-ФКЗ, от 30 дек. 2008 г. № 7-ФКЗ, от 5 февр. 2014 г. 28 № 2-ФКЗ, от 21 июля 2014 г. № 11-ФКЗ]. – Москва : Юрай, 2017. - ISBN 978-5-04-014029-3

2. Российская Федерация. Законы. Об Образовании : принят Государственной Думой 21 декабря2012 года. Одобрен Советом Федерации 26 декабря 2012 года - Москва, Эксмо, 2017 . - 350 с.

3. Российская Федерация. Законы. Трудовой кодекс Российской Федерации : принят Государственной Думой 21 декабря 2001 года. Одобрен Советом Федерации 26 декабря 2001 года // Доступ к СПС КонсультантПлюс

4. Федеральные государственные образовательные стандарты среднего профессионального образования // Доступ к СПС КонсультантПлюс

5. Журнал «Университетская наука» изд-во : СКФ БГТУ им. В.Г. Шухова, Минеральные Воды

3.2.4 Перечень ресурсов информационно-телекоммуникационной сети «Интернет» (далее – сеть «Интернет»), необходимых для освоения дисциплины

1. http://tu.tusur.ru/upload/posobia/s20.pdf
2. http://uchebnik.online/predprinimatelstvo-uchebnik/osnovyi-predprinimatelstva-uchebnik.html
3. http://www.academia-moscow.ru/ftp_share/_books/fragments/fragment_19564.pdf
4. http://ecsocman.edu.ru/text/19208131/
5. http://www.kodges.ru/48435organizaciyapredprinimatelskojdeyatelnosti.html

3.2.5 Перечень программного обеспечения, профессиональных баз данных и информационных справочных систем

Программное обеспечение:

1. Операционная система Windows 7 (License № 64080343 от 15.09.2014);
2.Офисный пакет приложений Microsoft Office 2007 (License № 43846774 от 25.02.2008).

Профессиональные базы данных и информационные справочные системы:

1. ИС «Техэксперт». Режим доступа из корпоративной сети университета: http://sk5-410-libte.at.urfu.ru/docs/

2. Портал информационно-образовательных ресурсов (http://study.ustu.ru)
3. Поисковые системы: Google (http://google.ru), Yandex (http://yandex.ru).
5. База нормативной технической документации (http://www.complexdoc.ru).
6. Поисковая система (http://www.freepatent.ru/).

4. КОНТРОЛЬ И ОЦЕНКА РЕЗУЛЬТАТОВ ОСВОЕНИЯ УЧЕБНОЙ ДИСЦИПЛИНЫ

Контроль и оценка результатов освоения дисциплины осуществляется преподавателем в процессе проведения тестирования, а также выполнения обучающимися индивидуальных заданий и исследований.

Результаты обучения (освоенные умения, усвоенные знания) **Результатом освоения учебной дисциплины являются следующие**	**Основные показатели оценки результата**	**Формы и методы контроля**
умения:		
- конструировать криптостойкие алгоритмы и протоколы;	Демонстрация умений по конструированию криптостойких алгоритмов и протоколов	опрос по индивидуальным заданиям; тестирование
- проводить анализ криптостойкости алгоритмов и протоколов	Демонстрация умений проводить анализ криптостойкости алгоритмов и протоколов	опрос по индивидуальным заданиям; тестирование
- создавать программы, реализующие алгоритмы и протоколы защищенной передачи данных;	Демонстрация умений создавать программы, реализующие алгоритмы и протоколы защищенной передачи данных	опрос по индивидуальным заданиям; оценка освоенных знаний в ходе выполнения контрольной работы тестирование
знания:		
- основные направления развития криптографии, теории информации и теории кодирования;	Демонстрация знаний основных направлений развития криптографии, теории информации и теории кодирования	опрос по индивидуальным заданиям; оценка освоенных знаний в ходе выполнения контрольной работы тестирование
- основные принципы построения кодов, криптосистем и крипто протоколов;	Демонстрация знаний основных принципов построения кодов, криптосистем и крипто протоколов	опрос по индивидуальным заданиям; оценка освоенных знаний в ходе выполнения контрольной работы тестирование
- основные методы анализа криптостойкости информационных систем;	Демонстрация знаний основных методов анализа криптостойкости информационных систем	опрос по индивидуальным заданиям; тестирование
- основные алгоритмы шифрования;	Демонстрация знаний основных алгоритмов шифрования	опрос по индивидуальным заданиям; оценка освоенных знаний в ходе выполнения контрольной работы тестирование
- основные протоколы защищенной передачи данных.	Демонстрация знаний основных протоколов защищенной передачи данных	опрос по индивидуальным заданиям; тестирование