

**Автономная некоммерческая организация высшего образования  
«Информационно-технологический университет»  
(АНО ВО ИТУ)**

УТВЕРЖДАЮ

Ректор АНО ВО ИТУ, Б.С. Лиджиев



«04» июня 2024 г.

**РАБОЧАЯ ПРОГРАММА ДИСЦИПЛИНЫ**

**Б1.В.ДЭ.02.02 СОВРЕМЕННАЯ КРИПТОГРАФИЯ И СТЕГАНОГРАФИЯ**

**Для направления подготовки:**

09.03.01 Информатика и вычислительная техника  
(уровень бакалавриата)

**Типы задач профессиональной деятельности:**

производственно-технологический

**Направленность (профиль):**

Информационные системы

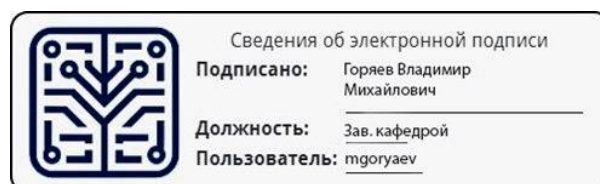
**Форма обучения:**

очная, очно-заочная, заочная

Разработчик: Горяев Владимир Михайлович, кандидат педагогических наук, заведующий кафедрой Математики и информационных технологий АНО ВО «Информационно-технологический университет».

Рабочая программа разработана в соответствии с требованиями ФГОС ВО 09.03.01 Информатика и вычислительная техника (уровень бакалавриата), утв. Приказом Министерства образования и науки РФ № 929 от 19.09.2017 г.

СОГЛАСОВАНО:  
Заведующий кафедрой  
Математики и информационных технологий  
канд. пед. наук, доцент Горяев В.М.



Протокол заседания кафедры № 01 от «04» июня 2024 г.

## 1. ЦЕЛЬ И ЗАДАЧИ ДИСЦИПЛИНЫ

**Цель освоения дисциплины:** сформировать знания, умения и компетенции в области современной криптографии и стеганографии.

**Задачи:**

- раскрыть особенности криптографических методов защиты информации и содержание базовых понятий криптографии;
- ознакомить с основными видами шифров;
- ознакомить с современными стандартами криптографической защиты;
- дать представление об атаках на криптографические системы;
- раскрыть основные направления современной криптографии и стеганографии.

## 2. МЕСТО ДИСЦИПЛИНЫ В СТРУКТУРЕ ОПОП

### 2.1. Место дисциплины в учебном плане:

**Блок:** Блок 1. Дисциплины (модули).

**Часть:** формируемая участниками образовательных отношений, элективные дисциплины.

**Осваивается (семестр):**

очная форма обучения – 6

очно-заочная форма обучения – 7

заочная форма обучения - 7

## 3. КОМПЕТЕНЦИИ, ФОРМИРУЕМЫЕ В РЕЗУЛЬТАТЕ ОСВОЕНИЯ ДИСЦИПЛИНЫ

**УК-2** - способен определять круг задач в рамках поставленной цели и выбирать оптимальные способы их решения, исходя из действующих правовых норм, имеющихся ресурсов и ограничений.

**ПК-2** - способен разрабатывать компоненты программных комплексов и баз данных в соответствии с требованиями технического задания, используя современные инструментальные средства и технологии программирования, оформлять программную и пользовательскую документацию в соответствии с принятыми стандартами.

## 4. РЕЗУЛЬТАТЫ ОСВОЕНИЯ ДИСЦИПЛИНЫ ОБУЧАЮЩИМСЯ

Код и наименование компетенции	Индикаторы достижения компетенции	Результаты обучения
<b>УК-2</b> Способен определять круг задач в рамках поставленной цели и выбирать оптимальные способы их решения, исходя из действующих правовых норм, имеющихся ресурсов и ограничений	<b>УК-2.2.</b> Выбирает оптимальный способ решения задач, учитывая действующие правовые нормы и имеющиеся условия, ресурсы и ограничения	<b>Знает:</b> методологию выбора оптимальных способов решения задач, учитывая действующие правовые нормы и имеющиеся условия, ресурсы и ограничения <b>Умеет:</b> определять круг задач, планировать и выбирать пути их решения, исходя из действующих правовых норм, имеющихся ресурсов и ограничений <b>Владеет:</b> способами решения конкретных задач в профессиональной деятельности, исходя из действующих норм, имеющихся ресурсов

<p><b>ПК-2</b> Способен разрабатывать компоненты программных комплексов и баз данных в соответствии с требованиями технического задания, используя современные инструментальные средства и технологии программирования, оформлять программную и пользовательскую документацию в соответствии с принятыми стандартами</p>	<p><b>ПК-2.1.</b> Выбирает современные инструментальные средства и технологии программирования для решения задач в профессиональной деятельности, оформляет программную и пользовательскую документацию в соответствии с принятыми стандартами</p>	<p><b>Знает:</b> основы программирования, современные структурные и объектно-ориентированные языки программирования, языки программирования и работы с базами данных <b>Умеет:</b> кодировать на языках программирования, использовать современные инструментальные средства и технологии программирования, разрабатывать пользовательскую документацию в соответствии с принятыми стандартами <b>Владеет:</b> навыками выбора языков и систем программирования при решении задач в профессиональной деятельности, средствами разработки программной и пользовательской документации</p>
--	--	--

## 5. ОБЪЕМ ДИСЦИПЛИНЫ И РАСПРЕДЕЛЕНИЕ ВИДОВ УЧЕБНОЙ РАБОТЫ ПО СЕМЕСТРАМ

Общая трудоемкость дисциплины «Современная криптография и стеганография» для обучающихся всех форм обучения, реализуемых в АНО ВО «Информационно-технологический университет» по направлению подготовки 09.03.01 Информатика и вычислительная техника составляет: 3 з.е. / 108 час.

Вид учебной работы	Всего число часов и (или) зачетных единиц (по формам обучения)		
	Очная	Очно-заочная	Заочная
<b>Аудиторные занятия</b>	54	32	12
<i>в том числе:</i>			
Лекции	18	10	4
Практические занятия	18	10	4
Лабораторные работы	18	12	4
<b>Самостоятельная работа</b>	54	76	92
<i>в том числе:</i>			
часы на выполнение КР / КП	-	-	-
<b>Промежуточная аттестация:</b>			
Вид	Зачет	Зачет	Зачет
Семестр	6	7	7
Трудоемкость (час.)	-	-	4
<b>Общая трудоемкость з.е. / час.</b>	<b>3 з.е. / 108 час.</b>		

## 6. СТРУКТУРА И СОДЕРЖАНИЕ ДИСЦИПЛИНЫ

Номер темы дисциплины	Количество часов (по формам обучения)											
	Очная				Очно-заочная				Заочная			
	Лекции	Практические занятия	Лабораторные работы	Самост. работа (в т.ч. КР / КП)	Лекции	Практические занятия	Лабораторные работы	Самост. работа (в т.ч. КР / КП)	Лекции	Практические занятия	Лабораторные работы	Самост. работа (в т.ч. КР / КП)
Тема 1	4	4	4	13	2	2	3	19	1	1	1	23
Тема 2	4	4	4	13	2	2	3	19	1	1	1	23
Тема 3	5	5	5	14	3	3	3	19	1	1	1	23
Тема 4	5	5	5	14	3	3	3	19	1	1	1	23
Итого (часов)	18	18	18	54	10	10	12	76	4	4	4	92
Форма контроля	Зачет				Зачет				Зачет			
<b>Всего по дисциплине</b>	<b>108 / 3 з.е.</b>											

### СОДЕРЖАНИЕ ТЕМ ДИСЦИПЛИНЫ

#### **Тема 1. Симметричные и асимметричные криптосистемы**

Основные классы симметричных криптосистем. Общие сведения о блочных шифрах. Генерирование блочных шифров. Алгоритмы блочного шифрования. Режимы применения блочных шифров. Поточковые шифры. Общие сведения о потоковых шифрах. Самосинхронизирующиеся шифры. Синхронные шифры. Примеры потоковых шифров.

Асимметричные системы шифрования. Криптосистема Эль-Гамала. Криптосистема, основанная на проблеме Диффи-Хеллмана. Криптосистема Ривеста-Шамира-Адлемана. Криптосистемы Меркля-Хеллмана и Хора-Ривеста. Криптосистемы, основанные на эллиптических кривых.

#### **Тема 2. Электронные цифровые подписи. Управление криптографическими ключами**

Алгоритмы электронной цифровой подписи. Цифровые подписи, основанные на асимметричных криптосистемах. Стандарт цифровой подписи DSS. Цифровые подписи, основанные на симметричных криптосистемах. Функции хэширования.

Система управления ключами. Управление ключами, основанное на системах с открытым ключом. Протокол обмена секретным ключом. Использование сертификатов. Протоколы аутентификации. Анонимное распределение ключей.

#### **Тема 3. Стеганографические системы**

Скрытие данных в неподвижных изображениях. Человеческое зрение и алгоритмы сжатия изображений. Скрытие данных в пространственной области. Скрытие данных в области преобразования.

Обзор стегоалгоритмов встраивания информации в изображения. Аддитивные алгоритмы. Стеганографические методы на основе квантования. Стегоалгоритмы, использующие фрактальное преобразование.

Скрытие данных в аудиосигналах. Скрытие данных в видеопоследовательностях. Современные стеганографические продукты.

#### **Тема 4. Современные направления в криптографии и криптоанализе**

Криптография в беспроводных сетях. Цифровая сотовая связь. Система безопасности GSM... Безопасность телефонных переговоров. Беспроводные сети Wi-Fi. Методы шифрования WEP и WPA. Программные продукты, использующие шифрование.

Криптография в «Интернете вещей». Квантовая криптография и квантовые вычисления. Криптография и технология блокчейн. Криптографическая защита биометрических данных. Другие актуальные и перспективные направления криптографии.

## **7. ПРИМЕРНАЯ ТЕМАТИКА КУРСОВЫХ РАБОТ**

Курсовая работа не предусмотрена

## **8. ФОНД ОЦЕНОЧНЫХ СРЕДСТВ ПО ДИСЦИПЛИНЕ:**

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: Фонд оценочных средств (материалов) по компетенциям представлен на сайте в разделе «Фонд оценочных средств (материалов)».

## **9. УЧЕБНО-МЕТОДИЧЕСКОЕ И ИНФОРМАЦИОННОЕ ОБЕСПЕЧЕНИЕ ДИСЦИПЛИНЫ:**

### **9.1. Рекомендуемая литература:**

- Прикладная стеганография / В. Г. Грибунин, В. Е. Костюков, А. П. Мартынов [и др.]; под редакцией В. Г. Грибунина, В. Е. Костюкова. — Саров: Российский федеральный ядерный центр – ВНИИЭФ, 2021. — 484 с. — ISBN 978-5-9515-0456-2. — Текст: электронный // Цифровой образовательный ресурс IPR SMART: [сайт]. — URL: <https://www.iprbookshop.ru/132624.html>
- Фороузан, Б. А. Криптография и безопасность сетей: учебное пособие / Б. А. Фороузан ; под редакцией А. Н. Берлина. — 4-е изд. — Москва: Интернет-Университет Информационных Технологий (ИНТУИТ), Ай Пи Ар Медиа, 2025. — 776 с. — ISBN 978-5-4497-0946-2. — Текст: электронный // Цифровой образовательный ресурс IPR SMART: [сайт]. — URL: <https://www.iprbookshop.ru/146352.html>
- Гисин, В. Б. Криптография и распределенные реестры: учебное пособие / В. Б. Гисин. — Москва: Прометей, 2022. — 186 с. — ISBN 978-5-00172-257-1. — Текст: электронный // Цифровой образовательный ресурс IPR SMART: [сайт]. — URL: <https://www.iprbookshop.ru/153506.html>

### **9.2. Перечень информационных технологий, используемых при осуществлении образовательного процесса по дисциплине (модулю), включая перечень лицензионного и свободно распространяемого программного обеспечения.**

АНО ВО «Информационно-технологический университет» обеспечен необходимым комплектом лицензионного и свободно распространяемого программного обеспечения, в том числе отечественного производства.

Программное обеспечение, необходимое для осуществления образовательного

процесса по дисциплине:

**Лицензионное программное обеспечение (в том числе, отечественного производства):**

Операционная система Windows Professional 10;

ПО браузер – приложение операционной системы, предназначенное для просмотра Web-страниц;

Цифровой образовательный сервис «Личная студия обучающегося» (отечественное ПО);

Цифровой образовательный сервис «Личный кабинет преподавателя» (отечественное ПО);

Платформа проведения вебинаров (отечественное ПО);

Платформа проведения аттестационных процедур с использованием каналов связи (отечественное ПО).

Информационная технология. Программа управления образовательным процессом.

**Свободно распространяемое программное обеспечение (в том числе отечественного производства):**

Мой Офис Веб-редакторы <https://edit.myoffice.ru> (отечественное ПО);

ПО OpenOffice.Org Calc - [http://qsp.su/tools/onlinehelp/about\\_license\\_gpl\\_russian.html](http://qsp.su/tools/onlinehelp/about_license_gpl_russian.html);

ПО OpenOffice.Org.Base [http://qsp.su/tools/onlinehelp/about\\_license\\_gpl\\_russian.html](http://qsp.su/tools/onlinehelp/about_license_gpl_russian.html);

ПО OpenOffice.org.Impress

[http://qsp.su/tools/onlinehelp/about\\_license\\_gpl\\_russian.html](http://qsp.su/tools/onlinehelp/about_license_gpl_russian.html)

ПО OpenOffice.Org Writer

[http://qsp.su/tools/onlinehelp/about\\_license\\_gpl\\_russian.html](http://qsp.su/tools/onlinehelp/about_license_gpl_russian.html)

ПО Open Office.org Draw

[http://qsp.su/tools/onlinehelp/about\\_license\\_gpl\\_russian.html](http://qsp.su/tools/onlinehelp/about_license_gpl_russian.html)

ПО «Блокнот» - стандартное приложение операционной системы (MS Windows, Android и т.д.), предназначенное для работы с текстами.

### **9.3. Перечень современных профессиональных баз данных, информационных справочных систем и ресурсов информационно-телекоммуникационной сети «Интернет»**

1. <https://ro-edu.ru/> - Медиалпортал «Российское образование»
2. <http://www.iprbookshop.ru> - Электронно-библиотечная система IPRSMART (ЭБС IPRSMART) –электронная библиотека по всем отраслям знаний
3. <https://www.elibrary.ru/> - электронно-библиотечная система eLIBRARY.RU, крупнейшая в России электронная библиотека научных публикаций
4. <http://www.consultant.ru/> - справочная правовая система КонсультантПлюс
5. <https://www.garant.ru/> - справочная правовая система Гарант
6. <https://gufo.me/> - справочная база энциклопедий и словарей
7. Официальный сайт оператора единого реестра российских программ для электронных вычислительных машин и баз данных в информационно-телекоммуникационной сети «Интернет» <https://reestr.digital.gov.ru/>
8. Web-технологии <https://htmlweb.ru/php/mysql.php>

## **10. МАТЕРИАЛЬНО-ТЕХНИЧЕСКОЕ ОБЕСПЕЧЕНИЕ ДИСЦИПЛИНЫ**

Описание материально-технической базы, необходимой для осуществления образовательного процесса по дисциплине представлено в Приложении 8 - Сведения о наличии оборудованных учебных кабинетов, объектов для проведения практических занятий ОПОП ВО по направлению подготовки 09.03.01 Информатика и вычислительная техника, направленность (профиль) «Информационные системы».

## 11. МЕТОДИЧЕСКИЕ РЕКОМЕНДАЦИИ ДЛЯ ОБУЧАЮЩИХСЯ ПО ОСВОЕНИЮ ДИСЦИПЛИНЫ

Изучение дисциплины проводится в форме лекций, практических и/или лабораторных занятий, организации самостоятельной работы обучающихся, консультаций.

Главное назначение лекции - обеспечить теоретическую основу обучения, развить интерес к учебной деятельности и конкретной учебной дисциплине, сформировать у обучающихся ориентиры для самостоятельной работы над учебной дисциплиной.

Основной целью практических и/или лабораторных занятий является обсуждение наиболее сложных теоретических вопросов, их методологическая и методическая проработка, выполнение практических заданий.

Самостоятельная работа с учебной, учебно-методической и научной литературой, дополняется работой с тестирующими системами, тренинговыми программами, с информационными базами, электронными образовательными ресурсами в электронной информационно-образовательной среде организации и сети Интернет.

Цель самостоятельной работы - подготовка современного компетентного специалиста и формирование способностей и навыков к непрерывному самообразованию и профессиональному совершенствованию.

Реализация поставленной цели предполагает решение следующих задач:

- качественное освоение теоретического материала по изучаемой дисциплине, углубление и расширение теоретических знаний с целью их применения на уровне межпредметных связей;
- систематизация и закрепление полученных теоретических знаний и практических навыков;
- формирование умений по поиску и использованию нормативной, правовой, справочной и специальной литературы, а также других источников информации;
- развитие познавательных способностей и активности, творческой инициативы, самостоятельности, ответственности и организованности;
- формирование самостоятельности мышления, способностей к саморазвитию, самообразованию, самосовершенствованию и самореализации;
- развитие научно-исследовательских навыков;
- формирование умения решать практические задачи (в профессиональной деятельности), используя приобретенные знания, способности и навыки.

Самостоятельная работа является неотъемлемой частью образовательного процесса.

Самостоятельная работа предполагает инициативу самого обучающегося в процессе сбора и усвоения информации, приобретения новых знаний, умений и навыков и ответственность его за планирование, реализацию и оценку результатов учебной деятельности. Процесс освоения знаниями при самостоятельной работе не обособлен от других форм обучения.

Самостоятельная работа по подготовке письменных работ должна:

- быть выполнена индивидуально (или являться частью коллективной работы);
- представлять собой законченную разработку (этап разработки), в которой анализируются актуальные проблемы по определенной теме и ее отдельных аспектов;
- отражать необходимую и достаточную компетентность автора;
- иметь учебную, научную и/или практическую направленность;

- быть оформлена структурно и логически последовательно;
- содержать краткие и четкие формулировки, убедительную аргументацию, доказательность и обоснованность выводов;
- соответствовать этическим нормам (правила цитирования и парафраз; ссылки на использованные библиографические источники; исключение плагиата, дублирования собственного текста и использования чужих работ).

### **11.1. Особенности организации образовательного процесса для обучающихся с ограниченными возможностями здоровья, инвалидов (детей-инвалидов) (в случае наличия таких категорий, обучающихся)**

Образовательный процесс включает в себя теоретическое обучение, все виды практик, воспитательную работу, мероприятия по комплексному сопровождению для обучающихся с ограниченными возможностями здоровья, инвалидов (детей-инвалидов) с учетом их возрастных и индивидуальных особенностей.

Образовательная программа может быть адаптирована для обучающихся с ограниченными возможностями здоровья, инвалидов (детей-инвалидов) (адаптивная образовательная программа). Адаптивная образовательная программа разрабатывается на основании личного заявления обучающегося (законного представителя) и рекомендаций психолого-медико-педагогической комиссии и/или справке медико-социальной экспертизы, индивидуальная программа реабилитации или абилитации.

При разработке адаптивной образовательной программы учитываются особые образовательные потребности обучающихся с ограниченными возможностями здоровья, инвалидов (детей-инвалидов), исходя из особенностей их психофизического развития, индивидуальных возможностей.

Обучающимся с ограниченными возможностями здоровья, инвалидам (детям-инвалидам) по их заявлению предоставляются специальные технические средства, программные средства и услуги ассистента (помощника), оказывающего необходимую техническую помощь.

При реализации адаптивной образовательной программы обучающимся с ограниченными возможностями здоровья, инвалидам (детям-инвалидам) предоставляются следующие возможности:

- использование специальных технических средств;
- обеспечение электронными образовательными ресурсами, использующими аудио сопровождение учебного материала;
- обеспечение электронными образовательными ресурсами с возможностью увеличения размера шрифта;
- обеспечение печатными образовательными ресурсами;
- особенности процедур аттестации.

При реализации адаптивной образовательной программы применяются следующие формы контроля и оценки результатов обучения обучающихся с ограниченными возможностями здоровья, инвалидов (детей-инвалидов) в зависимости от характера ограничений здоровья.

Для обучающихся с нарушением зрения:

- устная проверка: дискуссии, тренинги, круглые столы и др.;

- с использованием компьютера и специального программного обеспечения: работа с электронными образовательными ресурсами, тестирование, рефераты, курсовые проекты и др.;

- при возможности, письменная проверка с использованием шрифта Брайля, увеличенного шрифта, использование специальных технических средств: контрольные работы, тестирование, домашние задания, эссе, отчеты и др.

Для обучающихся с нарушением слуха:

- письменная проверка: контрольные, тестирование, домашние задания, эссе, отчеты и др.;

- с использованием компьютера и специального программного обеспечения: работа с электронными образовательными ресурсами, тестирование, рефераты, курсовые проекты и др.;

- при возможности, устная проверка с использованием специальных технических и программных средств, дискуссии, тренинги, круглые столы и др.

Для обучающихся с нарушением опорно-двигательного аппарата:

- письменная проверка с использованием специальных технических средств: контрольные работы, тестирование, домашние задания, эссе, отчеты и др.;

- устная проверка с использованием специальных технических средств: дискуссии, тренинги, круглые столы и др.;

- с использованием компьютера и специального программного обеспечения: работа с электронными образовательными ресурсами, тестирование, рефераты, курсовые проекты и др.

При проведении промежуточной аттестации по дисциплине обеспечивается соблюдение следующих общих требований:

- проведение аттестации для обучающихся с ограниченными возможностями здоровья, инвалидов (детей-инвалидов) в одной аудитории совместно с обучающимися, не имеющими инвалидности и ОВЗ, если это не создает трудностей для обучающихся с ограниченными возможностями здоровья, инвалидов (детей-инвалидов) и иных обучающихся при прохождении аттестации;

- присутствие в аудитории ассистента (помощника), оказывающего обучающимся с ограниченными возможностями здоровья, инвалидам (детям-инвалидам) необходимую техническую помощь с учетом их индивидуальных особенностей (занять рабочее место, передвигаться, прочесть и оформить задание, общаться с экзаменатором);

- обеспечение возможности беспрепятственного доступа обучающихся с ограниченными возможностями здоровья, инвалидов (детей-инвалидов) в аудиторию, спортивный зал, санитарные и другие вспомогательные помещения.

По письменному заявлению обучающегося с ограниченными возможностями здоровья, инвалидов (детей-инвалидов) продолжительность сдачи экзамена может быть увеличена по отношению к установленной продолжительности его сдачи:

- продолжительность сдачи экзамена, проводимого в письменной форме, - не более чем на 90 минут;

- продолжительность подготовки обучающегося к ответу на экзамене, проводимом в устной форме, - не более чем на 20 минут.

О необходимости обеспечения специальных условий для проведения аттестации обучающихся с ограниченными возможностями здоровья, инвалидов (детей-инвалидов),

обучающийся должен сообщить письменно не позднее, чем за 10 дней до начала аттестации. К заявлению прилагаются документы, подтверждающие наличие у обучающегося индивидуальных особенностей (при отсутствии указанных документов в организации).