Министерство науки и высшего образования Российской Федерации
Федеральное государственное бюджетное образовательное учреждение
высшего образования
**«Владимирский государственный университет
имени Александра Григорьевича и Николая Григорьевича Столетовых»
(ВлГУ)**

Институт информационных технологий и радиоэлектроники

УТВЕРЖДАЮ:
Директор института
_____ Галкин А. А.
«_26_» _августа_ 20_21_ г.

РАБОЧАЯ ПРОГРАММА ДИСЦИПЛИНЫ

«МЕТОДЫ И СРЕДСТВА КРИПТОГРАФИЧЕСКОЙ ЗАЩИТЫ ИНФОРМАЦИИ»

направление подготовки / специальность

10.03.01 «Информационная безопасность»
(код и наименование направления подготовки (специальности)

направленность (профиль) подготовки

**Безопасность автоматизированных систем
(по отраслям или в сфере профессиональной деятельности)**
(направленность (профиль) подготовки))

г. Владимир

2021 год

1. ЦЕЛИ ОСВОЕНИЯ ДИСЦИПЛИНЫ

Целями освоения дисциплины «Методы и средства криптографической защиты информации» являются обеспечение подготовки студентов в соответствии с требованиями ФГОС ВО 3++ и учебного плана по направлению 10.03.01 «Информационная безопасность», ознакомление студентов с основами теории двоичного кодирования, алгоритмами сжатия, помехоустойчивого кодирования. Дисциплина «Методы и средства криптографической защиты информации» рассматривается как теоретическая и прикладная дисциплина, дающая представления об основных математических и алгоритмических подходах, применяемых для хранения, передачи, исправления информации, представленной в двоичных кодах. Дисциплина посвящена изучению основ криптографии и криптографического анализа, применяемых к защите информации в информационных системах Обучаемые знакомятся с понятием шифров, симметричной и асимметричной криптографии, электронной подписью, хешированием и другими математическими объектами криптографии. Изучаются соответствующие криптографические стандарты, применяемые сегодня в защите информации в России и за рубежом. Подробно рассматриваются: стандарты RSA, DES, GOST1989, и другие. Также уделено внимание перспективным направлениям в криптографии: криптографические протоколы с разглашением и без разглашения, теория алгоритмической сложности и односторонних функций, схемы разделения секрета и некоторые их приложения в задачах идентификации и аутентификации

Задачами курса дисциплины являются: ознакомление с основами математической теории криптологии; приобретение навыков в практическом использовании, постановке и решении задач шифрования информации; понимание сути информационных процессов в криптографических системах; применение компьютеров для решения задач шифрования и дешифрования; разработка и использование математических и вычислительных моделей процессов шифрования информации, их оптимизация и выработка направлений совершенствования.

2. МЕСТО ДИСЦИПЛИНЫ В СТРУКТУРЕ ОПОП

Дисциплина «Методы и средства криптографической защиты информации» относится к обязательной части образовательной программы, код Б1.О.10 бакалавриата направления подготовки 10.03.01 «информационная безопасность». В учебном плане предусмотрены виды учебной деятельности, обеспечивающие синтез теоретических лекций, лабораторных работ и самостоятельной работы студентов. Курс тесно взаимосвязан с другими дисциплинами данного цикла.

3. ПЛАНИРУЕМЫЕ РЕЗУЛЬТАТЫ ОБУЧЕНИЯ ПО ДИСЦИПЛИНЕ

Планируемые результаты обучения по дисциплине, соотнесенные с планируемыми результатами освоения ОПОП (компетенциями и индикаторами достижения компетенций)

Формируемые компетенции (код, содержание компетенции)	Планируемые результаты обучения по дисциплине, в соответствии с индикатором достижения компетенции		Наименование оценочного средства
	Индикатор достижения компетенции *(код, содержание индикатора*	Результаты обучения по дисциплине	
ОПК-3 Способен использовать необходимые математические методы для решения задач	ОПК-3.1.1	Знает основные понятия теории информации (энтропия, взаимная информация, источники сообщений, каналы связи, коды)	Тестовые вопросы, КР
	ОПК-3.1.2	Знает понятие пропускной способности канала связи, прямую и обратную теоремы кодирования (без доказательства)	

профессиональной деятельности	ОПК-3.2.1	Знает основные методы оптимального кодирования источников информации (код Хаффмана) и помехоустойчивого кодирования каналов связи (линейные коды, циклические коды, код Хэмминга)	
	ОПК-3.2.2	Умеет вычислять теоретико-информационные характеристики источников сообщений и каналов связи (энтропия, взаимная информации, пропускная способность)	
	ОПК-3.3.1	Владеть общими проблемы криптологии, в сфере применения соответствующих задач, возникающих при построении информационных систем различного назначения, а также критерии информационных оценок функционирования этих систем	
ОПК-9 Способен применять средства криптографической и технической защиты информации для решения задач профессиональной деятельности	ОПК-9.1.1	Знать основные понятия и задачи криптографии, математические модели криптографических систем	
	ОПК-9.1.2	Знать основные виды средств криптографической защиты информации (СКЗИ), включая блочные и поточные системы шифрования, криптографические системы с открытым ключом, криптографические хеш-функции и криптографические протоколы	
	ОПК-9.1.3	Знать национальные стандарты Российской Федерации в области криптографической защиты информации и сферы их применения	
	ОПК-9.1.4	Знать основные положения (основополагающие теоремы) криптологии, вытекающие из теории симметричных и ассиметричных криптографических подходов, а также информационные критерии оценок функционирования криптографических систем	
	ОПК-9.2.1	Уметь разрабатывать и рассчитать характеристики криптографической защиты информационных систем в зависимости от назначения этих систем (количество информации, скорость передачи информации, пропускную способность каналов связи, требуемый объём памяти и др.)	
	ОПК-9.2.2	Уметь применять современные технологии криптографии в задачах обработки информации	
	ОПК-9.2.3	Уметь применять математические модели для оценки стойкости СКЗИ	
	ОПК-9.2.4	Уметь использовать СКЗИ в автоматизированных системах	
	ОПК-9.3.1	Владеть общими проблемы криптологии, в сфере применения соответствующих задач, возникающих при построении информационных систем различного назначения, а также критерии информационных оценок функционирования этих систем	

4. ОБЪЕМ И СТРУКТУРА ДИСЦИПЛИНЫ

Трудоемкость дисциплины составляет 11 зачетных единиц, 396 часов

Тематический план
форма обучения – очная

№ п/п	Наименование тем и/или разделов/тем дисциплины	Семестр	Неделя семестра	Контактная работа обучающихся с педагогическим работником				Самостоятельная работа	Формы текущего контроля успеваемости, форма промежуточной аттестации *(по семестрам)*
				Лекции	Практические занятия	Лабораторные работы	*в форме практической подготовки*		
1	Введение. Основные задачи криптологии. Криптография и криптографический анализ	4	1-2	4		4		4	
2	Открытый и закрытый тексты, ключ, основные свойства функции шифрования и дешифрования.	4	3-4	4		4		4	
3	Симметричные шифры. Группы подстановок и перестановок. Чистые шифры. Шифры Виженера и Вернама.	4	5-6	4		4		4	Рейтинг-контроль №1
4	Одноразовый блокнот. Теорема Шеннона об абсолютно стойком шифре.. Проблемы симметричной криптографии.	4	7-8	4		4		4	
5	Хеш - функции. Хеш - функции, устойчивые в слабом и сильном смысле по отношению к поиску коллизий.	4	9-10	4		4		4	
6	Блочные Шифры. Стандарты DES, GOST1989. Поточные шифры. Стандарт A5.	4	11-12	4		4		4	Рейтинг-контроль №2
7	Асимметричная криптография. Классы алгоритмической сложности. Сложность математических задач.	4	13-14	4		4		4	
8	Задачи факторизации и дискретного логарифма. Функция Эйлера. RSA. Электронная подпись.	4	15-16	4		4		4	
9	Криптографические протоколы. Протокол анонимных вычислений. Схемы разделения секрета. Криптография на эллиптических кривых	4	17-18	4		4		4	Рейтинг-контроль №3
Всего за 4 семестр:		**108**		**36**		**36**		**36**	**Зачет**
1	Чистые шифры. Шифры Виженера и Вернама.	5	1-2	4		4		9	
2	Принцип Керкхоффса.	5	3-4	4		4		9	

3	Хеш - функции. Хеш - функции, устойчивые в слабом и сильном смысле по отношению к поиску коллизий. Парадокс о днях рождения	5	5-6	4		4		9	Рейтинг-контроль №1
4	Блочные Шифры.	5	7-8	4		4		9	
5	Стандарт GOST1989. Поточные шифры. Стандарт A5.	5	9-10	4		4		9	
6	Сложность математических задач.	5	11-12	4		4		9	Рейтинг-контроль №2
7	Проблемы симметричной криптографии.	5	13-14	4		4		9	
8	Стандарты DES	5	15-16	4		4		9	
9	Односторонние функции	5	17-18	4		4		9	Рейтинг-контроль №3
Всего за 5 семестр:		**180**		**36**		**36**		**81**	**Экзамен (27)**
1	Криптографические протоколы.	6	1-2	4		4		1	
2	Протокол анонимных вычислений.	6	3-4	4		4		1	
3	Криптография на эллиптических кривых	6	5-6	4		4		1	Рейтинг-контроль №1
4	Электронная подпись.	6	7-8	4		4		1	
5	Функция Эйлера. RSA.	6	9-10	4		4		1	
6	Задачи факторизации и дискретного логарифма.	6	11-12	4		4		1	Рейтинг-контроль №2
7	Схемы разделения секрета	6	13-14	4		4		1	
8	Принцип Керкхоффса	6	15-16	4		4		1	
9	Примеры щифров. Шифр Цезаря, Полибия	6	17-18	4		4		1	Рейтинг-контроль №3
Всего за 6 семестр		**180**		**36**		**36**		**9**	**Экзамен (27)**
Наличие в дисциплине КП/КР		**Есть (5)**							
Итого по дисциплине		**468**		**108**		**108**		**198**	**Зачет Экзамен (27) Курсовая работа Экзамен (27)**

Содержание лекционных занятий по дисциплине

Темы лекций 4 семестр:

Раздел 1. Введение. Стандарты и функции криптографии

Тема 1. *Введение. Основные задачи криптологии. Криптография и криптографический анализ.* Основные задачи криптографии: Обеспечение конфиденциальности данных (предотвращение несанкционированного доступа к данным). Обеспечение целостности данных— гарантии того, что при передаче или хранении данные не были модифицированы пользователем, не имеющим на это права. Обеспечение аутентификации.

Тема 2. *Открытый и закрытый тексты, ключ, основные свойства функции шифрования и дешифрования.* Основной целью применения SSL сертификатов является шифрование данных, передаваемых на сервер от клиента и клиенту от сервера. Для обеспечения безопасности такого соединения современные браузеры используют алгоритм TLS, основанный на сертификатах формата X.509. Данный алгоритм применяет ассиметричное шифрование, чтобы создать ключ сессии для симмертичного шифрования. Последнее используется непосредственно для передачи данных после установления защищенного соединения.

Тема 3. *Симметричные шифры. Группы подстановок и перестановок. Чистые шифры. Шифры Виженера и Вернама.* Изучить алгоритмы симметричного шифрования информации DES и ГОСТ 28147-89. Познакомиться с критериями оценки свойств лавинного эффекта. Стандарты и функции криптографии

Тема 4. *Одноразовый блокнот. Теорема Шеннона об абсолютно стойком шифре.. Проблемы симметричной криптографии.* **Шифр Вернама** (англ. *Vernam cipher*) — система симметричного шифрования, изобретённая в 1917 году Гилбертом Вернамом Шифр является разновидностью криптосистемы одноразовых блокнотов. В нём используется булева функция «исключающее или». Шифр Вернама является примером системы с абсолютной криптографической стойкостью. При этом он считается одной из простейших криптосистем

Тема 5. *Хеш - функции. Хеш - функции, устойчивые в слабом и сильном смысле по отношению к поиску коллизий.* Изучить принципы работы «Crypton Word», «Crypton Excel», понять процедуры шифрования/дешифрования электронных документов, постановки электронной цифровой подписи (ЭЦП): 1. Проверить наличие ключа Novex Stealth в порте LPT на задней панели системного блока. Выполнить настройку эмулятора Crypton 2. Открыть программу MS Word. 3. Создать новый электронный документ или открыть любой имеющийся. Создать защищённый документ и поставить ЭЦП. 4. Ознакомиться с работой ПО мастер ключей шифрования 5. Ознакомиться с программой тестирования функций приложения Crypton API 6. Получить навыки работы с Crypton Disk

Раздел 2. Виды шифрования и протоколов.

Тема 1. *Блочные Шифры. Стандарты DES, GOST1989. Поточные шифры. Стандарт A5.* Изучить и реализовать режимы работы блочных шифров и схемы кратного шифрования для симметричных алгоритмов шифрования DES и ГОСТ28147-89. Режимами шифрования называют различные алгоритмы обработки данных, построенные на основе базового режима ECB. Криптографическая стойкость этих алгоритмов определяется в основном стойкостью базового режима. Однако, особенности различных режимов шифрования позволяют использовать блочный шифр для решения различных криптографических задач

Тема 2. *Асимметричная криптография. Классы алгоритмической сложности. Сложность математических задач.* Изучить математические основы криптографических методов защиты информации; основные алгоритмы симметричного и асимметричного шифрования данных; основы организации структуры криптосистем

Тема 3. *Криптографические протоколы. Протокол анонимных вычислений. Схемы разделения секрета. Криптография на эллиптических кривых.* Криптографический протокол (англ. *Cryptographic protocol*) — это абстрактный или конкретный протокол, включающий набор криптографических алгоритмов. В основе протокола лежит набор правил, регламентирующих использование криптографических преобразований и алгоритмов в информационных процессах. Функции, виды.

Темы лекций 5 семестр:

Раздел 1. Стандарты и функции криптографии

Тема 1. *Чистые шифры. Шифры Виженера и Вернама.* Шифр Виженера (фр. *Chiffre de Vigenère*) — метод полиалфавитного шифрования буквенного текста с использованием ключевого слова. Этот метод является простой формой многоалфавитной замены. Шифр Виженера изобретался многократно. Впервые этот метод описал Джовани Баттиста Белласо (итал. *Giovan Battista Bellaso*) в книге La cifra del. Sig. Giovan Battista Bellaso в 1553 году однако в XIX веке получил имя Блеза Виженера, французского дипломата. Метод прост для понимания и реализации, он является недоступным для простых методов криптоанализа. Хотя шифр легко понять и реализовать, на протяжении трех столетий он противостоял всем попыткам его сломать; чем и заработал имя le chiffre indéchiffrable (фр. *неразгаданный шифр*).

Многие люди пытались реализовать схемы шифрования, которые по сути являлись шифрами Виженера.

Тема 2. *Принцип Керкхоффса.* Прѝнцип Керкго́ффса — правило разработки криптографических систем, согласно которому в засекреченном виде держится только определённый набор параметров алгоритма, называемый ключом, а сам алгоритм шифрования должен быть открытым. Другими словами, при оценке надёжности шифрования необходимо предполагать, что противник знает об используемой системе шифрования всё, кроме применяемых ключей. Широко применяется в криптографии. Впервые данный принцип сформулировал в XIX веке голландский криптограф Огюст Керкгоффс

Тема 3. *Хеш - функции. Хеш - функции, устойчивые в слабом и сильном смысле по отношению к поиску коллизий. Парадокс о днях рождения*. Изучить принципы работы «Crypton Word», «Crypton Excel», понять процедуры шифрования/дешифрования электронных документов, постановки электронной цифровой подписи (ЭЦП): 1. Проверить наличие ключа Novex Stealth в порте LPT на задней панели системного блока. Выполнить настройку эмулятора Crypton 2. Открыть программу MS Word. 3. Создать новый электронный документ или открыть любой имеющийся. Создать защищённый документ и поставить ЭЦП. 4. Ознакомиться с работой ПО мастер ключей шифрования 5. Ознакомиться с программой тестирования функций приложения Crypton API 6. Получить навыки работы с Crypton Disk

Тема 4. *Электронная подпись.* Изучить принципы работы «Crypton Word», «Crypton Excel», понять процедуры шифрования/дешифрования электронных документов, постановки электронной цифровой подписи (ЭЦП): 1. Проверить наличие ключа Novex Stealth в порте LPT на задней панели системного блока. Выполнить настройку эмулятора Crypton 2. Открыть программу MS Word. 3. Создать новый электронный документ или открыть любой имеющийся. Создать защищённый документ и поставить ЭЦП. 4. Ознакомиться с работой ПО мастер ключей шифрования 5. Ознакомиться с программой тестирования функций приложения Crypton API 6. Получить навыки работы с Crypton Disk

Тема 5. *Функция Эйлера. RSA.* Получение навыков создания зашифрованного сообщения при помощи алгоритма шифрования RSA

Раздел 2. Виды шифрования и протоколов.

Тема 1. *Проблемы симметричной криптографии.* Симметри́чные криптосисте́мы (также симметричное шифрование, симметричные шифры) (англ. *symmetric-key algorithm*) — способ шифрования, в котором для шифрования и дешифрования применяется один и тот же криптографический ключ. До изобретения схемы асимметричного шифрования единственным существовавшим способом являлось симметричное шифрование. Ключ алгоритма должен сохраняться в тайне обеими сторонами, должны осуществляться меры по защите доступа к каналу, на всем пути следования криптограммы, или сторонами взаимодействия посредством криптообъектов, сообщений, если данный канал взаимодействия под грифом "Не для использования третьими лицами". Алгоритм шифрования выбирается сторонами до начала обмена сообщениями.

Тема 2. *Симметричная криптография.* симметричная криптография (или криптографические системы с открытым ключом) - криптографическая схема, функции которой заключаются в обеспечении возможности шифрования и/или электронной цифровой подписи, при которой один ключ (открытый) используется для шифрования сообщения или проверки цифровой подписи, а второй (закрытый, называемый также секретным) ключ используется для расшифрования сообщений и для создания цифровой подписи. Секретный и открытый ключи получателя связаны между собой однонаправленной функцией таким образом, что вычисление открытого ключа из секретного осуществляется за полиномиальное время, а вычисление секретного ключа по известному открытому является вычислительно сложной задачей. В данный раздел криптографии обычно включают и алгоритмы обмена ключами, так как они основываются на тех же математических принципах. Изучить математические основы

криптографических методов защиты информации; основные алгоритмы симметричного и асимметричного шифрования данных; основы организации структуры криптосистем

Тема 3. *Стандарты DES.* DES (англ. Data Encryption Standard) — алгоритм для симметричного шифрования, разработанный фирмой IBM и утверждённый правительством США в 1977 году как официальный стандарт (FIPS 46-3). В основе алгоритма лежит сеть Фейстеля с 16 циклами (раундами) и ключом, имеющим длину 56 бит. Размер ключа: 56 бит + 8 проверочных. Размер блока: 64 бит. Тип: Сеть Фейстеля. Число раундов: 16

Темы лекций 6 семестр:

Раздел 1. Введение. Стандарты и функции криптографии

Тема 1. *Криптографические протоколы.* Криптографический протокол (англ. Cryptographic protocol) — это абстрактный или конкретный протокол, включающий набор криптографических алгоритмов. В основе протокола лежит набор правил, регламентирующих использование криптографических преобразований и алгоритмов в информационных процессах.

Тема 2. *Протокол анонимных вычислений.* SSL (англ. *Secure Sockets Layer* — уровень защищённых сокетов) — криптографический протокол, который подразумевает более безопасную связь. Он использует асимметричную криптографию для аутентификации ключей обмена, симметричное шифрование для сохранения конфиденциальности, коды аутентификации сообщений для целостности сообщений. Протокол широко использовался для обмена мгновенными сообщениями и передачи голоса через IP (англ. *Voice over IP* — VoIP) в таких приложениях, как электронная почта, интернет-факс и др. В 2014 году правительство США сообщило об уязвимости в текущей версии протокола[1]. SSL должен быть исключён из работы в пользу TLS (см. CVE-2014-3566). SSL изначально разработан компанией *Netscape Communications* для добавления протокола HTTPS в свой веб-браузер Netscape Navigator. Впоследствии на основании протокола SSL 3.0 был разработан и принят стандарт RFC, получивший имя TLS.

Тема 3. *Криптография на эллиптических кривых.* Эллиптическая криптография — раздел криптографии, который изучает асимметричные криптосистемы, основанные на эллиптических кривых над конечными полями. ... Использование эллиптических кривых для создания криптосистем было независимо друг от друга предложено Нилом Коблицем и Виктором Миллером в 1985 году.

Тема 4. *Задачи факторизации и дискретного логарифма*. Дискретное логарифмирование (DLOG) — задача обращения функции в некоторой конечной мультипликативной группе. Наиболее часто задачу дискретного логарифмирования рассматривают в мультипликативной группе кольца вычетов или конечного поля, а также в группе точек эллиптической кривой над конечным полем. Эффективные алгоритмы для решения задачи дискретного логарифмирования в общем случае неизвестны.

Тема 5. *Схемы разделения секрета*. Схема разделения секрета - криптографическая схема, позволяющая разделить секрет между участниками группы, при этом каждый участник получает долю секрета, а исходный секрет стирается. Воссоздать **секрет** может определенная коалиция участников

Раздел 2. Виды шифрования и протоколов.

Тема 1. *Принцип Керкхоффса.* Прúнцип Керкгóффса — правило разработки криптографических систем, согласно которому в засекреченном виде держится только определённый набор параметров алгоритма, называемый ключом, а сам алгоритм шифрования должен быть открытым. Другими словами, при оценке надёжности шифрования необходимо предполагать, что противник знает об используемой системе шифрования всё, кроме применяемых ключей. Широко применяется в криптографии. Впервые данный принцип сформулировал в XIX веке голландский криптограф Огюст Керкгоффс

Тема 2. *Примеры щифров. Шифр Цезаря, Полибия***.** Шифр Цезаря -- это вид шифра подстановки, в котором каждый символ в открытом тексте заменяется буквой, находящейся на некоторое постоянное число позиций левее или правее него в алфавите. Например, в шифре со сдвигом 3, А была бы заменена на Г, Б станет Д, и так далее. Шифр назван в честь римского императора Гая Юлия Цезаря, использовавшего его для секретной переписки со своими генералами. Шаг шифрования, выполняемый шифром Цезаря, часто включается как часть более сложных схем, таких как шифр Виженера, и все еще имеет современное приложение в системе ROT13. Как и все моноалфавитные шифры, шифр Цезаря легко взламывается и не имеет практически никакого применения на практике.

Содержание лабораторных занятий по дисциплине

Темы лабораторных работ 4 семестр:

Лабораторная работа №1. Тема 1: Ассиметричная криптография.

Лабораторная работа №2. Тема 2: Функции Эйлера. RSA.

Лабораторная работа №3. Тема 3: Стандарты DES.

Лабораторная работа №4. Тема 4: Блочные шифры.

Темы лабораторных работ 5 семестр:

Лабораторная работа №1. Тема 1: Шифр Цезаря.

Лабораторная работа №2. Тема 2: Шифрование файлов. Четыре криптопримитива.

Лабораторная работа №3. Тема 3: Многораундовое шифрование.

Лабораторная работа №4. Тема 4: Криптографические тесты (NIST).

Темы лабораторных работ 6 семестр:

Раздел 1. Генерация ключей.

Лабораторная работа №1. Тема 1: Хэш-функция. Электронная подпись.

Лабораторная работа №2. Тема 2: Генератор псевдослучайных последовательностей.

Лабораторная работа №3. Тема 3: Генерация ключей.

Лабораторная работа №4. Тема 4: Арифметика с длинными целыми.

5. ОЦЕНОЧНЫЕ СРЕДСТВА ДЛЯ ТЕКУЩЕГО КОНТРОЛЯ УСПЕВАЕМОСТИ, ПРОМЕЖУТОЧНОЙ АТТЕСТАЦИИ ПО ИТОГАМ ОСВОЕНИЯ ДИСЦИПЛИНЫ И УЧЕБНО-МЕТОДИЧЕСКОЕ ОБЕСПЕЧЕНИЕ САМОСТОЯТЕЛЬНОЙ РАБОТЫ СТУДЕНТОВ

5.1. Текущий контроль успеваемости

Вопросы рейтинг-контроля №1 для семестра 4:

- Основные задачи криптографии и криптоанализа. Понятие криптопреобразования. Краткая справка по истории возникновения и развития, и современному криптографии.
- Понятие несимметрии математических операций и трудоемкость элементарных математических операций.
- Понятие криптосистемы.
- Типы криптосистем.
- Криптосистемы с открытым ключом

Вопросы рейтинг-контроля №2 для семестра 4:

- Основные математические понятия для конечного поля, характеристика поля.
- Возможность построения конечного поля с необходимым числом элементов.
- Мультипликативная группа конечного поля. Образующие. Дискретный логарифм

- Порядок многочлена над конечным полем.
- Конструкция конечного поля из pn элементов.
- Псевдослучайные последовательности и их применение в криптографии.

Вопросы рейтинг-контроля №3 для семестра 4:

- Псевдослучайные последовательности и их применение в криптографии.
- Алгебра последовательностей над конечным полем.
- Линейные рекуррентные последовательности над конечным полем.
- Аннулирующие многочлены.
- Регистр сдвига.
- Экспоненциальный открытый ключ.

Вопросы рейтинг-контроля №1 для семестра 5:

- Свойства решений линейного рекуррентного уравнения.
- Суммы с характерами.
- Максимальные линейные рекуррентные последовательности как псевдослучайные последовательности.

Вопросы рейтинг-контроля №2 для семестра 5:

- Аннулирующие многочлены.
- Регистр сдвига.
- Экспоненциальный открытый ключ.
- Вычисление дискретного логарифма.
- Число появлений наборов фиксированной длины на полном периоде рекуррентной последовательности.

Вопросы рейтинг-контроля №3 для семестра 5:

- Дискретные отображения и признаки хаотичности числовых рядов.
- Методы криптографии на основе сортировки детерминировано-хаотических рядов.
- Методы криптографии на основе парных сравнений чисел в детерминировано-хаотических числовых рядах.
- Стеганография.

Вопросы рейтинг-контроля №1 для семестра 6:

- Понятие электронной подписи. Необходимость электронной подписи в криптосистемах с открытым ключом.
- Математическая теория групп как основа современных криптосистем.
- Дискретные отображения и признаки хаотичности числовых рядов.
- Аннулирующие многочлены.

Вопросы рейтинг-контроля №2 для семестра 6:

- Алгебра последовательностей над конечным полем.
- Линейные рекуррентные последовательности над конечным полем.
- Конструкция конечного поля из pn элементов.
- Свойства решений линейного рекуррентного уравнения.
- Суммы с характерами.
- Максимальные линейные рекуррентные последовательности как псевдослучайные последовательности.

Вопросы рейтинг-контроля №3 для семестра 6:

- Оценки и критерии сложности алгоритмов криптографии.
- Криптоанализ и алгоритмические неразрешимые проблемы.
- Особенности хаотических систем.
- Вычисление дискретного логарифма.
- Число появлений наборов фиксированной длины на полном периоде рекуррентной последовательности.

5.2. Промежуточная аттестация по итогам освоения дисциплины

Примерный перечень вопросов к зачету 4 семестр

- Основные задачи криптографии и криптоанализа. Понятие криптопреобразования. Краткая справка по истории возникновения и развития, и современному криптографии.
- Понятие несимметрии математических операций и трудоемкость элементарных математических операций.
- Понятие криптосистемы.
- Типы криптосистем.
- Криптосистемы с открытым ключом
- Понятие электронной подписи. Необходимость электронной подписи в криптосистемах с открытым ключом.
- Математическая теория групп как основа современных криптосистем.
- Основные математические понятия для конечного поля, характеристика поля.
- Свойства решений линейного рекуррентного уравнения.
- Суммы с характерами.
- Максимальные линейные рекуррентные последовательности как псевдослучайные последовательности.
- Дискретные отображения и признаки хаотичности числовых рядов.
- Аннулирующие многочлены.
- Аннулирующие многочлены.
- Регистр сдвига.
- Экспоненциальный открытый ключ.
- Вычисление дискретного логарифма.
- Число появлений наборов фиксированной длины на полном периоде рекуррентной последовательности.

Примерный перечень вопросов к экзамену 5 семестр

- Возможность построения конечного поля с необходимым числом элементов.
- Мультипликативная группа конечного поля. Образующие. Дискретный логарифм
- Группы перестановок и подстановок в криптографии. Двойственность. Теорема о сохранении энтропии для шифров подстановки и перестановки.
- Определение криптографических систем по Шеннону. Примеры шифров по Шеннону.
- Шифр Вижженера (Гаммирование). Взлом Гаммирования.
- Шифр Вернама. Одноразовый блокнот. Теорема об абсолютно стойком шифре.
- Классы сложности алгоритмов и задач. Примеры.
- Односторонние функции. Задачи-кандидаты в односторонние функции.
- Функции Эйлера и ее свойства. Теорема Эйлера и теорема Ферма.
- Факторизация целого числа.
- Порядок многочлена над конечным полем.
- Конструкция конечного поля из pn элементов.
- Псевдослучайные последовательности и их применение в криптографии.

- Алгебра последовательностей над конечным полем.
- Линейные рекуррентные последовательности над конечным полем.
- Конструкция конечного поля из pn элементов.
- Псевдослучайные последовательности и их применение в криптографии.
- Алгебра последовательностей над конечным полем.
- Линейные рекуррентные последовательности над конечным полем.
- Аннулирующие многочлены.
- Регистр сдвига.
- Экспоненциальный открытый ключ.
- Вычисление дискретного логарифма.
- Число появлений наборов фиксированной длины на полном периоде рекуррентной последовательности.

Примерный перечень вопросов к экзамену 6 семестр

- Свойства решений линейного рекуррентного уравнения.
- Суммы с характерами.
- Максимальные линейные рекуррентные последовательности как псевдослучайные последовательности.
- Дискретные отображения и признаки хаотичности числовых рядов.
- Методы криптографии на основе сортировки детерминировано-хаотических рядов.
- Методы криптографии на основе парных сравнений чисел в детерминировано-хаотических числовых рядах.
- Стеганография.
- Оценки и критерии сложности алгоритмов криптографии.
- Криптоанализ и алгоритмические неразрешимые проблемы.
- Особенности хаотических систем.
- Дискретный логарифм в конечных полях. Протокол Диффи-Хеллмана.
- Алгоритм RSA.
- Электронная подпись в ассиметричных схемах и ее свойства. С хеш функциями и без.
- Хеш функции и их свойства. Криптографические хеш-функции.
- Криптографические протоколы.
- Интераполяция многочленами. Теорема о существовании и единственности многочлена. Схема разделения секрета Шамира.
- Электронные деньги. Неотслеживаемость. Схема Шаума-Педерсана.
- Стандарты DES и ГОСТ Блочных шифров. Архитектурный и сравнительный анализ шифров.
- Блочные шифры. Режимы работ блочных шифров.
- Потоковые шифры.
- Криптографические модели безопасности. Модель симметричного шифрования, ассиметричного и модель Долев-Яо.

5.3. Самостоятельная работа обучающегося.

Примерные темы курсовой работы 5 семестр

1. Программная реализация шифров замены.
2. Программная реализация шифров перестановки.
3. Программная реализация шифра Плейфера.
4. Программная реализация шифра Хилла.
5. Разработка шифра, основанного на композиции шифра замены и перестановки, с оценкой его криптостойкости.
6. Анализ криптостойкости блочных криптосистем (ГОСТ 28147-89, DES, IDEA, AES).

7. Алгоритм электронной цифровой подписи на основе решения системы сравнений.
8. Анализ методов сокращения длины электронной цифровой подписи.
9. Алгоритмы коллективной электронной цифровой подписи.
10. Алгоритмы композиционной электронной цифровой подписи.
11. Сравнительный анализ современных программных, программно-аппаратных и аппаратных средств криптографической защиты информации.
12. Разработка схемы криптографического генератора, основанного на комбинировании LFSR-генераторов, с оценкой его качества.
13. Разработка схемы криптографического генератора, основанного на комбинировании конгруэнтных генераторов, с оценкой его качества.
14. Оценка качества криптографических генераторов, основанных на алгоритмах Фибоначчи.
15. Алгоритмы слепой электронной цифровой подписи. (СЛИВКА)
16. Сравнительный анализ алгоритмов формирования хэш-функций.
17. Сравнительный анализ современных криптосистем с открытым ключом.
18. Сравнительный анализ криптографических протоколов распределения ключей.
19. Разработка системы аутентификации пользователей сети передачи данных

Вопросы и задания для самостоятельной работы студентов 4 семестр:

- Какие основные модели цифровых автоматов используются в криптографии?
- Особенности функционирования и взаимодействия цифровых автоматов в криптографических системах.
- Одномерные и многомерные дискретные отображения, примеры;
- Методы минимизации и их сопоставительный анализ?
- Сложность алгоритмов криптографии. Критерии и оценки;

Вопросы и задания для самостоятельной работы студентов 5 семестр:

- Алгоритмы, универсальные алгоритмические системы, достоинства и недостатки;
- Основные понятия и определения, эквивалентность алгоритмов.
- Временная и емкостная сложность алгоритмов.
- Особенности многоядерных процессоров.
- Сопоставительный анализ

Вопросы и задания для самостоятельной работы студентов 6 семестр:

- Основные соотношения затрат памяти и времени.
- Автоматы на основе дискретного отображения Лоренца, достоинства и недостатки;
- Автоматы на основе отображений TentMap и Хенона, сопоставительный анализ.
- Сопоставительный анализ алгоритмов криптоанализа, оценки сложности;
- Перспективы криптоанализа и алгоритмически неразрешимы проблемы.

6. УЧЕБНО-МЕТОДИЧЕСКОЕ И ИНФОРМАЦИОННОЕ ОБЕСПЕЧЕНИЕ ДИСЦИПЛИНЫ

6.1. Книгообеспеченность

Наименование литературы: автор, название, вид издания, издательство	Год издания	КНИГООБЕСПЕЧЕННОСТЬ
		Наличие в электронном каталоге ЭБС
Основная литература		
Котов, Ю. А. Криптографические методы защиты информации: стандартные шифры. Шифры с открытым ключом : [16+] / Ю. А. Котов. – Новосибирск: Новосибирский государственный технический университет, 2017. – 67 с.– ISBN 978-5-7782-3411-6	2017	https://biblioclub.ru/index.php?page=book&id=574782 (дата обращения: 14.09.2021)

Майстренко, Н. В. Основы теории информации и криптографии: учебное электронное издание / Н. В. Майстренко, А. В. Майстренко. – Тамбов: Тамбовский государственный технический университет (ТГТУ), 2018. – 81 с. – ISBN 978-5-8265-1950-9	2018	https://biblioclub.ru/index.php?page=book&id=570354 (дата обращения: 14.09.2021)
Фороузан, Б. А. Математика криптографии и теория шифрования: учебное пособие: [16+] / Б. А. Фороузан. – 2-е изд., испр. – Москва: Национальный Открытый Университет «ИНТУИТ», 2016. – 511 с. – ISBN 978-5-9963-0242-0	2016	https://biblioclub.ru/index.php?page=book&id=428998 (дата обращения: 14.09.2021)
Лапонина, О. Р. Криптографические основы безопасности: учебное пособие: [16+] / О. Р. Лапонина. – Москва: Национальный Открытый Университет «ИНТУИТ», 2016. – 244 с.– ISBN 5-9556-00020-5	2016	https://biblioclub.ru/index.php?page=book&id=429092 (дата обращения: 14.09.2021)
Котов, Ю. А. Приложения шифров: криптоанализ: [16+] / Ю. А. Котов; Новосибирский государственный технический университет. – Новосибирск: Новосибирский государственный технический университет, 2019. – 76 с. – ISBN 978-5-7782-3902-9	2019	https://biblioclub.ru/index.php?page=book&id=575479 (дата обращения: 14.09.2021)
Дополнительная литература		
Кнауб, Л. В. Теоретико-численные методы в криптографии: учебное пособие / Л. В. Кнауб, Е. А. Новиков, Ю. А. Шитов; Сибирский федеральный университет. – Красноярск: Сибирский федеральный университет (СФУ), 2011. – 160 с. – ISBN 978-5-7638-2113-7	2011	https://biblioclub.ru/index.php?page=book&id=229582 (дата обращения: 14.09.2021)
Аграновский, А. В. Практическая криптография: алгоритмы и их программирование: [16+] / А. В. Аграновский, Р. А. Хади. – Москва: СОЛОН-ПРЕСС, 2009. – 256 с. – ISBN 5-98003-002-6	2009	https://biblioclub.ru/index.php?page=book&id=117663 (дата обращения: 14.09.2021)

6.2. Периодические издания

1. Журнал «Вопросы защиты информации». Режим доступа: http://i-vimi.ru/editions/detail.php?SECTION_ID=155/;
2. Журнал "Information Security/Информационная безопасность". Режим доступа: http://www.itsec.ru/insec-about.php.

6.3. Интернет-ресурсы

1. Образовательный сервер кафедры ИЗИ.– Режим доступа: http://edu.izi.vlsu.ru
2. Информационная образовательная сеть.- Режим доступа: http://ien.izi.vlsu.ru
3. Внутривузовские издания ВлГУ.– Режим доступа: http://e.lib.vlsu.ru/
4. ИНТУИТ. Национальный открытый университет.– Режим доступа: http://www.intuit.ru/

7. МАТЕРИАЛЬНО-ТЕХНИЧЕСКОЕ ОБЕСПЕЧЕНИЕ ДИСЦИПЛИНЫ

Занятия проводятся в следующих аудиториях ВлГУ (корпус №2) по адресу г. Владимир, ул. Белоконской, д. 3.

ауд. 408-2, Лекционная аудитория, количество студенческих мест – 50, площадь 60 м2, оснащение: мультимедийное оборудование (интерактивная доска Hitachi FX-77WD, проектор BenQ MX 503 DLP 2700ANSI XGA), ноутбук Lenovo Idea Pad B5045.

ауд. 427а-2, лаборатория сетевых технологий, количество студенческих мест – 14, площадь 36 м2, оснащение: компьютерный класс с 8 рабочими станциями Core 2 Duo E8400 с выходом в Internet, 3 маршрутизатора Cisco 2800 Series, 6 маршрутизаторов Cisco 2621, 6 коммутаторов Cisco Catalyst 2960 Series, 3 коммутатора Cisco Catalyst 2950 Series, коммутатор Cisco Catalyst Express 500 Series, проектор BenQ MP 620 P, экран настенный рулонный. Лицензионное программное обеспечение: операционная система Windows 7 Профессиональная, офисный

пакет приложений Microsoft Office Профессиональный плюс 2007, бесплатно распространяемое программное обеспечение: линейка интегрированных сред разработки Visual Studio Express 2012, программный продукт виртуализации Oracle VM VirtualBox 5.0.4, симулятор сети передачи данных Cisco Packet Tracer 7.0, интегрированная среда разработки программного обеспечения IntelliJ IDEA Community Edition 15.0.3.

ауд. 427б-2, УНЦ «Комплексная защита объектов информатизации», количество студенческих мест – 15, площадь 52 м2, оснащение: компьютерный класс с 7 рабочими станциями Alliance Optima P4 с выходом в Internet, коммутатор D-Link DGS-1100-16 мультимедийный комплект (проектор Toshiba TLP X200, экран настенный рулонный), прибор ST-031P «Пиранья-Р» многофункциональный поисковый, прибор «Улан-2» поисковый, виброакустический генератор шума «Соната АВ 1М», имитатор работы средств нелегального съема информации, работающих по радиоканалу «Шиповник», анализатор спектра «GoodWill GSP-827», индикатор поля «SEL SP-75 Black Hunter», устройство блокирования работы систем мобильной связи «Мозайка-3», устройство защиты телефонных переговоров от прослушивания «Прокруст 2000», диктофон Edic MINI Hunter, локатор «Родник-2К» нелинейный, комплекс проведения акустических и виброакустических измерений «Спрут мини-А», видеорегистратор цифровой Best DVR-405, генератор Шума «Гном-3»,учебно-исследовательский комплекс «Сверхширокополосные беспроводные сенсорные сети» (Nano Xaos), сканирующий приемник «Icom IC-R1500», анализатор сетей Wi-Fi Fluke AirCheck с активной антенной. Лицензионное программное обеспечение: Windows 8 Профессиональная, офисный пакет приложений Microsoft Office Профессиональный плюс 2010, бесплатно распространяемое программное обеспечение: линейка интегрированных сред разработки Visual Studio Express 2012, инструмент имитационного моделирования AnyLogic 7.2.0 Personal Learning Edition, интегрированная среда разработки программного обеспечения IntelliJ IDEA Community Edition 14.1.4.

Рабочую программу составил: доцент кафедры ИЗИ к.ф-м.н. Александров А.В

Рецензент: Заместитель руководителя РАЦ ООО «ИнфоЦентр» к.т.н. Вертилевский Н.В

Программа рассмотрена и одобрена на заседании кафедры ИЗИ

Протокол № 1 от 16.06.21 года
Заведующий кафедрой д.т.н., профессор /М.Ю. Монахов/

Рабочая программа рассмотрена и одобрена на заседании учебно-методической комиссии направления 10.03.01 «Информационная безопасность»

Протокол № 1 от 26.06.21 года
Председатель комиссии д.т.н., профессор /М.Ю. Монахов/

ЛИСТ ПЕРЕУТВЕРЖДЕНИЯ
РАБОЧЕЙ ПРОГРАММЫ ДИСЦИПЛИНЫ

Рабочая программа одобрена на 2022 / 2023 учебный год

Протокол заседания кафедры № 14 от 28.06.22 года

Заведующий кафедрой д.т.н., профессор /М.Ю. Монахов/
(ФИО, подпись)

Рабочая программа одобрена на 20____ / 20____ учебный год

Протокол заседания кафедры № _____ от _____ года

Заведующий кафедрой д.т.н., профессор /М.Ю. Монахов/
(ФИО, подпись)

Рабочая программа одобрена на 20____ / 20____ учебный год

Протокол заседания кафедры № _____ от _____ года

Заведующий кафедрой д.т.н., профессор /М.Ю. Монахов/
(ФИО, подпись)

Рабочая программа одобрена на 20____ / 20____ учебный год

Протокол заседания кафедры № _____ от _____ года

Заведующий кафедрой д.т.н., профессор /М.Ю. Монахов/
(ФИО, подпись)

ЛИСТ РЕГИСТРАЦИИ ИЗМЕНЕНИЙ

в рабочую программу дисциплины

Методы и средства криптографической защиты информации

образовательной программы направления подготовки *10.03.01 Информационная безопасность*

Номер изменения	Внесены изменения в части/разделы рабочей программы	Исполнитель ФИО	Основание (номер и дата протокола заседания кафедры)
1			
2			

Заведующий кафедрой _____/М.Ю. Монахов/__

Подпись *ФИО*