



Основная профессиональная образовательная программа
01.03.01 Математика
(Математика, алгоритмы и анализ данных)

Министерство науки и высшего образования Российской Федерации

ИВАНОВСКИЙ ГОСУДАРСТВЕННЫЙ УНИВЕРСИТЕТ

Центр подготовки специалистов в сфере информационной безопасности и
противодействия техническим средствам разведки

ОДОБРЕНО:

Руководитель ОП

(подпись) Ю.А. Хашина

«_1_» сентября_2022 г.

Рабочая программа дисциплины

Методы и средства криптографической защиты информации

Уровень высшего образования:	бакалавриат
Квалификация выпускника:	бакалавр
Направление подготовки:	01.03.01 Математика
Направленность (профиль) образовательной программы:	Математика, алгоритмы и анализ данных



1. Цели освоения дисциплины

Целью освоения дисциплины «Методы и средства криптографической защиты информации» является изучение основных направлений обеспечения безопасности процессов хранения, передачи, обработки, распространения информации.

2. Место дисциплины в структуре ОП

Настоящая дисциплина «Методы и средства криптографической защиты информации» относится к обязательной части учебного плана, изучается на 3-м курсе в 1 семестре. Курс опирается на следующие курсы: «Организационное и правовое обеспечение информационной безопасности», «Алгебраические основы криптографии».

3. Планируемые результаты обучения по дисциплине

3.1. Компетенции, формированию которых способствует дисциплина

При освоении дисциплины формируются следующие компетенции в соответствии с ФГОС ВО по данному направлению подготовки:

а) общепрофессиональные (ОПК): нет

б) профессиональные (ПК):

ПК-1 Способен выявлять актуальные научные проблемы в своей области специализации и решать их под руководством специалистов более высокой квалификации

ПК-3. Способен проводить работы по проектированию программного обеспечения

3.2. Перечень планируемых результатов обучения по дисциплине, соотнесенных с индикаторами достижения формируемых компетенций

В результате освоения дисциплины обучающийся должен:

Знать:

- основные понятия и задачи криптографии, математические модели криптографических систем;
- основные виды средств криптографической защиты информации (СКЗИ), включая блочные и поточные системы шифрования, криптографические системы с открытым ключом, криптографические хеш-функции и криптографические протоколы;
- национальные стандарты Российской Федерации в области криптографической защиты информации и сферы их применения;

Уметь:

- использовать СКЗИ для решения задач профессиональной деятельности

Иметь практический опыт/Иметь навыки:

- методами синтеза и анализа криптографических систем и протоколов, закономерностями построения сложных криптосистем;
- навыками эксплуатации криптографических протоколов и схем, получивших широкое применение в качестве инструментария в системах электронных платежей и систем документооборота в электронной коммерции.

4. Объем и содержание дисциплины

Объем дисциплины составляет 4 зачетные единицы (144 академических часа).

4.1. Содержание дисциплины по разделам (темам), соотнесенное с видами и трудоемкостью занятий лекционно-семинарского типа

Объем иной контактной работы и самостоятельной работы обучающегося по дисциплине указан в учебном плане образовательной программы.



Основная профессиональная образовательная программа

01.03.01 Математика

(Математика, алгоритмы и анализ данных)

№ п/п	Разделы (темы) дисциплины	Семестр	Виды занятий, их объем (в ак. часах, по очной форме обучения)		Формы текущего контроля успеваемости (по очной форме обучения)
			Занятия лекцион- ного типа	Занятия семинар- ского типа	Формы промежуточной аттестации
1.	Вводное занятие	5	2		Входная диагностика: тест с последующим обсуждением результатов. Список вопросов, интересующих студента по содержанию дисциплины (сдается в письменном виде)
2.	Место криптографических методов в защите информации	5	4	4	Обсуждение результатов практической работы
3.	Математическое описание базовых блочных алгоритмов зашифровывания	5	6	6	Обсуждение результатов практической работы
4.	Защита информации с помощью криптосистем	5	6	6	Обсуждение результатов практической работы
5.	Методы распределения ключей	5	6	6	Обсуждение результатов практической работы
6.	Стандарты в области криптографической защиты информации	5	4	4	Обсуждение результатов практической работы
7.	Применение СКЗИ в целях решения типовых задач защиты информации	5	6	4	Обсуждение результатов практической работы
8.	Заключительное занятие	5	2	2	Оценка контрольной работы
Итого за семестр:			36	32	Экзамен
Итого по дисциплине:			36	32	

4.2. Развернутое описание содержания дисциплины по разделам (темам)

Тема №1. Вводное занятие

Введение в проблематику дисциплины, представление рабочей программы, осмысление требований к организации процесса обучения, самостоятельной работы и форм аттестации

Тема №2. Место криптографических методов в защите информации.

Математические модели простейших шифров. Понятие о шифрах замены и перестановки, блочных и поточных шифрах. Основные требования к шифрам в связи с возможными угрозами к защищаемой информации.

Тема №3. Математическое описание базовых блочных алгоритмов зашифровывания

Математическое описание базовых блочных алгоритмов зашифровывания AES и ГОСТ 28147-89. Реализация поточных шифрсистем с помощью блочных шифров. Описание стандартных режимов шифрования и сравнение показателей помехоустойчивости для них. Задачи противостояния случайным и целенаправленным помехам.

Тема №4. Защита информации с помощью криптосистем

Защита информации с помощью криптосистем с открытым ключом. Понятие однонаправленной функции с секретом (ОФС). Примеры кандидатов на OFC. Понятие о системе шифрования с открытым ключом. Криптосистема RSA. Задачи защиты информации, решаемые с помощью OFC: обеспечение конфиденциальности, аутентичности сообщения и отправителя, доказательство авторства и другие. Понятие криптографической хеш-функции. Понятие



криптографического протокола. Простейшие криптографические протоколы, использующие асимметричное шифрование.

Тема №5. Методы распределения ключей

Основные методы распределения ключей. Предварительное распределение ключей. Пересылка ключей. Открытое распределение ключей. Схема разделения секрета. Теоретическая стойкость шифров. Основные требования к шифрам. Совершенные шифры. Теорема К. Шеннона о минимальных совершенных шифрах.

Тема №6. Стандарты в области криптографической защиты информации

Национальные стандарты Российской Федерации в области криптографической защиты информации и сферы их применения. Нормативное регулирование разработки, производства и применения средств криптографической защиты информации (СКЗИ), в том числе электронной цифровой подписи.

Тема №7. Применение СКЗИ в целях решения типовых задач защиты информации

Применение СКЗИ в целях решения типовых задач защиты информации: обеспечение конфиденциальности хранимой информации, конфиденциальности информационного обмена, аутентификация и взаимная аутентификация участников информационного взаимодействия, обеспечение функционирования удостоверяющих центров.

Тема №8. Заключительное занятие

Подведение и анализ промежуточных результатов освоения дисциплины

5. Образовательные технологии

Организация учебного процесса осуществляется в форме лекций, практических занятий и индивидуальной самостоятельной работы студентов.

Учебный процесс по дисциплине «Методы и средства криптографической защиты информации» основан на использовании следующих инновационных образовательных технологий:

1. Технология проблемного обучения – основные темы курса на лекциях и практических занятиях раскрываются через постановку и последующее разрешение проблемы создания алгоритма решения задачи и ее разрешение в виде функционирующей программы.
2. Технология тестового контроля качества образования – в процессе и по завершении теоретического обучения выполняется компьютерное тестирование.
3. Информационно-компьютерные технологии – применяются при выполнении практических работ, самостоятельной внеаудиторной подготовке в виде самотестирования по сети Internet и использования учебных материалов в электронной форме.
4. Технология смешанного обучения.

6. Учебно-методическое обеспечение самостоятельной работы обучающихся

Методика преподавания учебной дисциплины решает следующие основные задачи:

- определяет задачи обучения студентов по дисциплине;
- научно обосновывает содержание учебной программы, намечает последовательность ее изучения в комплексе с другими дисциплинами;
- определяет пути реализации принципов обучения при изучении дисциплины, формы и методы обучения;
- вырабатывает требования к методической подготовке преподавателей;
- изучает историю методики преподавания дисциплины;
- внедряет передовой опыт обучения;
- вырабатывает рекомендации по воспитанию обучаемых в процессе изучения дисциплины.

В соответствии с этими задачами осуществляется отбор научного материала, его систематизация и переработка в интересах развития и совершенствования содержания учебной дисциплины.



Методика разработана применительно к утвержденной рабочей программе для студентов с учетом требований Государственного образовательного стандарта высшего образования по направлению подготовки 090303 «Прикладная информатика», и вооружает преподавателей необходимыми знаниями, способствует их внедрению в практику обучения и воспитания студентов.

Выбор методов проведения занятий обусловлен учебными целями, содержанием учебного материала, временем, отводимым на занятия.

На занятиях в тесном сочетании применяется несколько методов, один из которых выступает ведущим. Он определяет построение и вид занятий.

На лекциях излагаются лишь основные, имеющие принципиальное значение и наиболее трудные для понимания и усвоения теоретические и практические вопросы.

Теоретические знания, полученные студентами на лекциях и при самостоятельном изучении курса по литературным источникам, закрепляются при выполнении практических работ.

Целями проведения практических работ являются:

- приобретение практических навыков работы с методами и средствами защиты криптографической защиты информации;
- контроль самостоятельной работы студентов по освоению курса;
- обучение навыкам профессиональной деятельности.

Цели практических работ достигаются наилучшим образом в том случае, если им предшествует определенная подготовительная внеаудиторная работа. Поэтому преподаватель обязан довести до всех студентов график выполнения практических работ с тем, чтобы они могли заниматься целенаправленной самостоятельной работой.

Работы рекомендуется выполнять в той последовательности, в которой они написаны, потому что в некоторых работах используются элементы, полученные в предыдущей работе.

На занятиях со студентами должны широко использоваться разнообразные средства обучения, способствующие более полному и правильному пониманию темы лекции или практического занятия, а также выработке практических навыков по работе с ППО.

К средствам обучения студентов относятся:

- речь преподавателя;
- технические средства обучения: персональные компьютеры с установленным прикладным программным обеспечением;
- учебники, учебные пособия, лекции в электронном виде.

Полностью весь методический материал по обеспечению самостоятельной работы студентов приводится в Приложении 1 к РП.

7. Характеристика оценочных средств для текущего контроля успеваемости и промежуточной аттестации обучающихся по дисциплине

Для контроля усвоения материала дисциплины «Методы и средства криптографической защиты информации» предусмотрен текущий и промежуточный контроль. Текущий контроль основан на анализе результатов выполнения практических работ и собеседовании по их темам. Промежуточный контроль заключается в сдаче экзамена по дисциплине.

Для проведения зачетов (экзаменов) в письменной или тестовой форме разрабатывается перечень вопросов, утверждаемый заведующим кафедрой. В перечень включаются вопросы из различных разделов курса, позволяющие проверить и оценить теоретические знания студентов и умение применять их для решения практических задач.

Зачет (экзамен) в письменной форме проводится одновременно для всех студентов академической группы. Время выполнения задания составляет не более одного академического часа.



При проведении зачета (экзамена) в письменной форме оценка выставляется на основе правил, принятых кафедрой, которые должны быть сообщены студентам до начала зачетной (экзаменационной) сессии.

Аналогичные правила могут быть заложены в программы компьютерного тестирования.

При контроле знаний в устной форме преподаватель использует метод индивидуального собеседования, в ходе которого обсуждает со студентом один или несколько вопросов из учебной программы. При необходимости могут быть предложены дополнительные вопросы, задачи и примеры. По окончании ответа на вопросы преподаватель объявляет студенту результаты сдачи зачета (экзамена).

8. Учебно-методическое и информационное обеспечение дисциплины

Основная литература:

1. Майстренко, Н. В. Основы теории информации и криптографии: учебное электронное издание : учебное пособие / Н. В. Майстренко, А. В. Майстренко. – Тамбов : Тамбовский государственный технический университет (ТГТУ), 2018. – 81 с. : табл., граф., схем., ил. – Режим доступа: по подписке. – URL: <https://biblioclub.ru/index.php?page=book&id=570354> (дата обращения: 04.12.2022). – Библиогр. в кн. – ISBN 978-5-8265-1950-9. – Текст : электронный.
2. 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. : ил., схем. – (Основы информационных технологий). – Режим доступа: по подписке. – URL: <https://biblioclub.ru/index.php?page=book&id=428998> (дата обращения: 04.12.2022). – Библиогр. в кн. – ISBN 978-5-9963-0242-0. – Текст : электронный.
3. 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. – Режим доступа: по подписке. – URL: <https://biblioclub.ru/index.php?page=book&id=229582> (дата обращения: 04.12.2022). – ISBN 978-5-7638-2113-7. – Текст : электронный.

Дополнительная литература:

1. Аграновский, А. В. Практическая криптография: алгоритмы и их программирование : учебное пособие : [16+] / А. В. Аграновский, Р. А. Хади. – Москва : СОЛОН-ПРЕСС, 2009. – 256 с. – (Аспекты защиты). – Режим доступа: по подписке. – URL: <https://biblioclub.ru/index.php?page=book&id=117663> (дата обращения: 04.12.2022). – ISBN 5-98003-002-6. – Текст : электронный.
2. Лидовский, В. В. Основы теории информации и криптографии: курс : учебное пособие : [16+] / В. В. Лидовский ; Национальный Открытый Университет "ИНТУИТ". – Москва : Интернет-Университет Информационных Технологий (ИНТУИТ), 2007. – 125 с. : табл., схем. – Режим доступа: по подписке. – URL: <https://biblioclub.ru/index.php?page=book&id=234148> (дата обращения: 04.12.2022). – Текст : электронный.

Ресурсы информационно-телекоммуникационной сети «Интернет»:

Система электронной поддержки образовательного процесса «Мой университет»
<https://uni.ivanovo.ac.ru>

Профессиональные базы данных и информационно-справочные системы:

ЭБС «Университетская библиотека онлайн» www.biblioclub.ru;
<http://lib.ivanovo.ac.ru/index.php/polnotekstovye-resursy/ebs-universitetskaya-biblioteka>



Электронная библиотека ИвГУ <http://lib.ivanovo.ac.ru/index.php/polnotekstovye-resursy/elibnew>

Электронный каталог НБ ИвГУ <http://lib.ivanovo.ac.ru/index.php/ek>

СПС «КонсультантПлюс» <http://www.consultant.ru/>

Программное обеспечение: операционная система Microsoft Windows, пакет офисных программ Microsoft Office и(или) LibreOffice, интернет-браузер Microsoft Edge и(или) Yandex Browser.

9. Материально-техническое обеспечение дисциплины

Учебные аудитории:

- для проведения занятий лекционного типа с комплектом специализированной учебной мебели и техническими средствами обучения, служащими для предоставления учебной информации большой аудитории;

- для проведения занятий семинарского типа, консультаций, текущего контроля и промежуточной аттестации с комплектом специализированной учебной мебели и техническими средствами обучения.

Лаборатория, оснащенная лабораторным оборудованием, комплектом специализированной учебной мебели и техническими средствами обучения.

Помещение для самостоятельной работы, оснащенное комплектом специализированной учебной мебели, компьютерной техникой с возможностью подключения к сети «Интернет» и обеспечением доступа в ЭИОС.

Демонстрационное оборудование и учебно-наглядные пособия для занятий лекционного типа, обеспечивающие тематические иллюстрации:

Автор(ы) рабочей программы дисциплины: Агупова Н.С., специалист

Программа рассмотрена и утверждена на заседании центра подготовки специалистов в сфере информационной безопасности и противодействия техническим средствам разведки

«_1_» сентября 2022 г., протокол № 1

Программа обновлена

протокол заседания центра ПСвСИБиПТСР № _____ от «_____» _____ 20__ г.

Согласовано:

Руководитель ОП _____ / Зарубин И.А.
(подпись)

Программа обновлена

протокол заседания центра ПСвСИБиПТСР № _____ от «_____» _____ 20__ г.

Согласовано:

Руководитель ОП _____ / Зарубин И.А.
(подпись)

Программа обновлена

протокол заседания центра ПСвСИБиПТСР № _____ от «_____» _____ 20__ г.

Согласовано:

Руководитель ОП _____ / Зарубин И.А.
(подпись)