МИНИСТЕРСТВО НАУКИ И ВЫСШЕГО ОБРАЗОВАНИЯ РОССИЙСКОЙ ФЕДЕРАЦИИ

федеральное государственное бюджетное образовательное учреждение высшего образования «Казанский национальный исследовательский технический университет им. А.Н. Туполева-КАИ»
Лениногорский филиал

УТВЕРЖДАЮ
Директор ЛФ КНИТУ-КАИ
_____ Р.А. Шамсутдинов
«25» апреля 2022 г.

РАБОЧАЯ ПРОГРАММА

дисциплины (модуля)

Б1.В.ДВ.01.02 Реализация спецификации криптографических сообщений
(индекс и наименование дисциплины по учебному плану)

Квалификация: *магистр*

Форма обучения: *очная*

Направление подготовки: *09.04.02 Информационные системы и технологии*

Направленность (профиль): *Безопасность информационных систем*

Лениногорск 2022

Рабочая программа дисциплины (модуля) разработана в соответствии с требованиями федерального государственного образовательного стандарта высшего образования - магистратура по направлению подготовки 09.04.02 Информационные системы и технологии, утвержденного приказом Министерства образования и науки Российской Федерации от 19 сентября 2017г. № 917.

Разработчик(и):
Сагдатуллин А.М., к.т.н., доцент кафедры МиИТ
(ФИО, ученая степень, ученое звание) *(подпись)*

Денисов О.В., к.т.н., старший преподаватель кафедры МиИТ
(ФИО, ученая степень, ученое звание) *(подпись)*

Рабочая программа утверждена на заседании кафедры МиИТ от «19» апреля 2022 г., протокол № 8.

/Заведующий кафедрой МиИТ
Думлер Е.Б., к.т.н.
(ФИО, ученая степень, ученое звание) *(подпись)*

Рабочая программа дисциплины (модуля):	Наименование Подразделения	Дата	№ протокола	Подпись
ОДОБРЕНА	на заседании кафедры МиИТ	19.04.2022	№ 8	Руководитель ОП А.М. Сагдатуллин
ОДОБРЕНА	Учебно-методическая комиссия ЛФ КНИТУ-КАИ	21.04.2022	№ 8	Председатель УМК З.И.Аскарова
СОГЛАСОВАНА	Научно-техническая библиотека	21.04.2022		Библиотекарь А.Г. Страшнова

1 ИСХОДНЫЕ ДАННЫЕ И КОНЕЧНЫЙ РЕЗУЛЬТАТ ИЗУЧЕНИЯ ДИСЦИПЛИНЫ (МОДУЛЯ)

1.1 Цель изучения дисциплины (модуля)

Целью освоения дисциплины является получение обучающимися систематизированных теоретических знаний о базовых принципах и методах реализации спецификаций криптографических сообщений, принципах построения алгоритмов шифрования.

1.2 Задачи дисциплины (модуля)

Задачами освоения дисциплины являются:

- освоение типовых приемов криптографии и построения шифрующих алгоритмов;
- привитие базовых навыков построения криптографических сообщений и разработки программ, реализующих криптоалгоритмы.

1.3 Место дисциплины (модуля) в структуре ОП ВО

Дисциплина относится к части, формируемой участниками образовательных отношений, Блока 1. Дисциплины (модули) образовательной программы и является элективной дисциплиной, определяющей ее предметно-тематическое содержание – направленность.

1.4 Объем дисциплины (модуля) и виды учебной работы

Объем дисциплины (модуля) в зачетных единицах с указанием количества академических часов, выделенных на контактную работу обучающихся с преподавателем (по видам учебных занятий) и на самостоятельную работу обучающихся представлены в таблице 1.1

Таблица 1.1

Объем дисциплины (модуля) для очной формы обучения

Семестр	Общая трудоемкость дисциплины (модуля), в ЗЕ/час	*Виды учебной работы, в т.ч., проводимые с использованием ЭО и ДОТ*											
		Контактная работа обучающихся с преподавателем по видам учебной работы (аудиторная работа)							***Самостоятельная работа обучающегося (внеаудиторная работа)***				
		Лекции/ в т.ч. в форме практической подготовки	Лабораторные работы/ в т.ч. в форме практической подготовки	Практические занятия/ в т.ч. в форме практической подготовки	Курсовая работа (консультация, защита)	Курсовой проект (консультации, защита)	Консультации перед экзаменом	Контактная работа на промежуточной аттестации	Курсовая работа (подготовка)/ в т.ч. в форме практической подготовки	Курсовой проект (подготовка)/ в т.ч. в форме практической подготовки	Проработка учебного материала (самоподготовка)/ в т.ч. в форме практической подготовки	Подготовка к промежуточной аттестации	Форма промежуточной аттестации
4	5 ЗЕ/180	16/8	16/16		-	-	-	2,3	-	-	112/50	33,7	Экзамен
Итого	5 ЗЕ/180	16/8	16/16		-	-	-	2,3	-	-	112/50	33,7	Экзамен

1.5 Перечень планируемых результатов обучения по дисциплине (модулю)

Процесс изучения дисциплины направлен на формирование компетенций, представленных в таблице 1.2.

Таблица 1.2

Формируемые компетенции

Код компетенции	Наименование компетенции	Индикаторы достижения компетенций	Планируемые результаты обучения
ПК-3	Способен выполнять работы по проектированию и созданию и сопровождению системного программного обеспечения и его компонент	ИД-1$_{ПК-3}$ – выполняет работы по проектированию архитектуры системного программного обеспечения; ИД-2$_{ПК-3}$ – разрабатывает программное обеспечение на основе выбранной архитектуры; ИД-3$_{ПК-3}$ – проектирует и	**Знает** принципы криптографии и распространенные алгоритмы шифрования **Умеет** выполнять шифрование сообщений с помощью распространенных алгоритмов шифрования

		разрабатывает компоненты программного обеспечения	**Владеет** навыками разработки шифрующего программного обеспечения

2 СОДЕРЖАНИЕ ДИСЦИПЛИНЫ (МОДУЛЯ)

2.1 Структура дисциплины (модуля)

Содержание дисциплины (модуля), структурированное по темам (разделам), с указанием отведенного на них количества академических часов и видов учебной работы приведены в таблице 2.1.

Таблица 2.1

Разделы дисциплины (модуля) и виды учебной работы

Наименование тем (разделов) дисциплины (модуля)	Всего (час)	Контактная работа обучающихся с преподавателем по видам учебных занятий (в час)				Самостоятельная работа (проработка учебного материала), выполнение курсовой работы /проекта, подготовка к ПА, самоподготовка.
		Лекции	Лабораторные работы	Практические занятия	КР, КП, ПА, консультация	
4 семестр						
1 Основные понятия и определения	18	2	2			14
2 Блочные шифры	18	2	2			14
3 Генераторы псевдослучайных чисел	18	2	2			14
4 Криптографические хэш-функции	18	2	2			14
5 Асимметричные криптосистемы	18	2	2			14
6 Распространение ключей	18	2	2			14
7 Разделение секрета	18	2	2			14
8 Примеры систем защиты	18	2	2			14
Промежуточная аттестация (экзамен)	36				2,3	33,7
Итого за семестр	**180**	**16**	**16**		**2,3**	**145,7**

2.2 Содержание разделов дисциплины (модуля)

1 Основные понятия и определения.

Модели систем передачи информации. Классификация. Симметричные и асимметричные криптосистемы. Шифры замены и перестановки. Примеры современных криптографических примитивов. Методы криптоанализа и типы атак. Минимальные длины ключей. Классические шифры. Моноалфавитные шифры. Шифр Цезаря. Аддитивный шифр перестановки. Аффинный шифр. Биграммные шифры замены. Полиграммный шифр замены Хилла. Шифр гаммирования Виженера.

2 Блочные шифры.

SP-сети. Проект «Люцифер». Ячейка Фейстеля. Шифр DES. ГОСТ 28147-89. Стандарт шифрования AES. Состояние, ключ шифрования и число раундов. Операции в поле. Операции одного раунда шифровани. Процедура расширения ключа. Шифр «Кузнечик». Режимы работы блочных шифров. Электронная кодовая книга. Сцепление блоков шифртекста. Обратная связь по выходу. Обратная связь по шифрованному тексту. Счётчик. Некоторые свойства блочных шифров. Обратимость схемы Фейстеля. Схема Фейстеля без s-блоков. Лавинный эффект. Двойное и тройное шифрования.

3 Генераторы псевдослучайных чисел.

Линейный конгруэнтный генератор. РСЛОС. КСГПСЧ. Генератор BBS. КСГПСЧ на основе РСЛОС. Генераторы с несколькими регистрами сдвига. Генераторы с нелинейными преобразованиями. Мажоритарные генераторы, шифр A5/1.

4 Криптографические хэш-функции.

ГОСТ Р 34.11-94. Хэш-функция «Стрибог». Имитовставка. Коллизии в хэш-функциях. Вероятность коллизии. Комбинации хэш-функций. Когда вредно хешировать. Blockchain (цепочка блоков). Централизованный blockchain с доверенным центром. Централизованный blockchain с недоверенным центром. Децентрализованный blockchain. Механизм внесения изменений в протокол.

5 Асимметричные криптосистемы.

Криптосистема RSA. Шифрование. Электронная подпись. Семантическая безопасность шифров. Выбор параметров и оптимизация. Криптосистема Эль-Гамаля. Шифрование. Электронная подпись. Криптостойкость. Эллиптические кривые. ECIES. Российский стандарт ЭП ГОСТ Р 34.10-2001. Длины ключей. Инфраструктура открытых ключей. Иерархия удостоверяющих центров. Структура сертификата X.509

6 Распространение ключей.

Симметричные протоколы. Протокол Wide-Mouth Frog. Протокол Yahalom. Протокол Нидхема — Шрёдера. Протокол «Kerberos». Трёхпроходные протоколы. Тривиальный вариант. Бесключевой протокол Шамира. Криптосистема Мэсси — Омуры. «Криптосистемы-протоколы». Протокол Диффи — Хеллмана. Протокол Эль-Гамаля. Протокол MTI/A(0). Протокол Station-to-Station. Схемы с доверенным центром. Схема Жиро. Схема Блома. Асимметричные протоколы. Протокол Деннинга — Сакко. Протокол DASS. Протокол By — Лама. Квантовые протоколы. Протокол BB84. Протокол B92 (BB92). Модификация Lo05. Общие недостатки квантовых протоколов.

7 Разделение секрета.

Пороговые схемы. Схема Блэкли. Схема Шамира. (N, N)-схема. Распределение по коалициям. Схема для нескольких коалиций. Схема разделения секрета Брикелла.

8 Примеры систем защиты.

Система Kerberos для локальной сети. Pretty Good Privacy. Протокол SSL/TLS. Протокол «рукопожатия». Протокол записи. Защита IPsec на сетевом уровне. Протокол создания ключей IKE. Таблица защищённых связей. Транспортный и туннельный режимы. Протокол шифрования и аутентификации ESP. Протокол аутентификации AH. Защита персональных данных в мобильной связи. GSM (2G). UMTS (3G).

2.3 Курсовая работа (курсовой проект)

Не предусмотрено учебным планом.

3 ОЦЕНОЧНЫЕ МАТЕРИАЛЫ И МЕТОДИЧЕСКИЕ РЕКОМЕНДАЦИИ ПО ОСВОЕНИЮ ДИСЦИПЛИНЫ (МОДУЛЯ)

Текущий контроль успеваемости обеспечивает оценивание хода освоения дисциплины (модуля).

Промежуточная аттестация обеспечивает оценивание промежуточных результатов обучения по дисциплине (модулю).

Комплект оценочных материалов представляет собой совокупность оценочных средств (комплекс заданий различного типа с ключами правильных ответов, включая критерии оценки), используемых при проведении оценочных процедур (текущего контроля, промежуточной аттестации) с целью оценивания достижения обучающимися результатов обучения по дисциплине (модулю).

Комплект оценочных материалов (текущего контроля и промежуточной аттестации), необходимых для оценивания результатов освоения дисциплины (модуля) представлен в виде отдельного документа по дисциплине (модулю) и хранится на кафедре-разработчике в бумажном или электронном виде.

3.1 Оценка успеваемости обучающихся

Текущий контроль успеваемости и промежуточная аттестация по дисциплине (модулю) осуществляется в соответствии с балльно-рейтинговой системой по 100-балльной шкале. Пересчет суммы баллов в традиционную оценку представлен в таблице 3.1.

Таблица 3.1

Шкала оценки на промежуточной аттестации

Выражение в баллах	Словесное выражение при форме промежуточной аттестации – экзамен
от 86 до 100	Отлично
от 71 до 85	Хорошо
от 51 до 70	Удовлетворительно
до 51	Не удовлетворительно

4 ОБЕСПЕЧЕНИЕ ДИСЦИПЛИНЫ (МОДУЛЯ)

4.1 Учебно-методическое и информационное обеспечение дисциплины (модуля)

4.1.1 Основная литература

1. Краковский, Ю. М. Методы защиты информации [Электронный ресурс]: учебное пособие для вузов / Ю. М. Краковский. — 3-е изд., перераб. — СПб: Лань, 2021. — 236 с. — Текст: электронный // Лань: электронно-библиотечная система. — URL: https://e.lanbook.com/book/156401

2. Каширская, Е. Н. Криптографические системы [Электронный ресурс]: учебное пособие / Е. Н. Каширская, А. П. Кушнир. — М.: РТУ МИРЭА, 2021. — 66 с. — Текст: электронный // Лань: электронно-библиотечная система. — URL: https://e.lanbook.com/book/182424

3. Васильева, И. Н. Криптографические методы защиты информации [Электронный ресурс]: учебник и практикум для вузов / И. Н. Васильева. — М.: Издательство Юрайт, 2022. — 349 с. — (Высшее образование). — Текст: электронный // Образовательная платформа Юрайт [сайт]. — URL: https://urait.ru/bcode/489919

4. Иванов, М. А. Криптографические методы защиты информации в компьютерных системах и сетях [Электронный ресурс]: учебное пособие / М. А. Иванов, И. В. Чугунков. — М.: НИЯУ МИФИ, 2012. — 400 с. — Текст: электронный // Лань: электронно-библиотечная система. — URL: https://e.lanbook.com/book/75810

5. Запечников, С. В. Криптографические методы защиты информации [Электронный ресурс]: учебник для вузов / С. В. Запечников, О. В. Казарин, А. А. Тарасов. — М.: Издательство Юрайт, 2022. — 309 с. — (Высшее образование). — Текст: электронный // Образовательная платформа Юрайт [сайт]. — URL: https://urait.ru/bcode/489487

4.1.2 Дополнительная литература

1 Корниенко, А. А. Криптографические протоколы [Электронный ресурс]: учебное пособие / А. А. Корниенко, М. Л. Глухарев. — СПб: ПГУПС, 2020. — 74 с. — Текст: электронный // Лань: электронно-библиотечная система. — URL: https://e.lanbook.com/book/191009

2. Гатченко, Н. А. Криптографическая защита информации [Электронный ресурс]:учебное пособие / Н. А. Гатченко, А. С. Исаев, А. Д. Яковлев. — СПб: НИУ ИТМО, 2012. — 142 с. — Текст: электронный // Лань: электронно-библиотечная система. — URL: https://e.lanbook.com/book/40849

3. Каширская, Е. Н. Криптографический анализ и методы защиты информации [Электронный ресурс]: учебное пособие / Е. Н. Каширская. — М.: РТУ МИРЭА, 2020. — 91 с. — Текст: электронный // Лань: электронно-библиотечная система. — URL: https://e.lanbook.com/book/163861

4. Криптографическая защита информации [Электронный ресурс]: учебное пособие / С. О. Крамаров, О. Ю. Митясова, С. В. Соколов [и др.] ; под ред. С. О. Крамарова. — М.: РИОР: ИНФРА-М, 2021. — 321 с. — (Высшее образование). - Текст: электронный. - URL: https://znanium.com/catalog/product/1153156

5. Аверченков, В. И. Криптографические методы защиты информации [Электронный ресурс]: учебное пособие / В. И. Аверченков, М. Ю. Рытов, С. А. Шпичак. — 2-е изд. — М.: ФЛИНТА, 2017. — 215 с. — Текст: электронный // Лань: электронно-библиотечная система. — URL: https://e.lanbook.com/book/92914

6. Рябко, Б. Я. Криптографические методы защиты информации [Электронный ресурс]: учебное пособие / Б. Я. Рябко, А. Н. Фионов. — 2-е изд., стер. — М.: Горячая линия-Телеком, 2017. — 230 с. — Текст: электронный // Лань: электронно-библиотечная система. — URL: https://e.lanbook.com/book/111097

4.1.3 Методические материалы

1. Методические указания к выполнению лабораторных работ по дисциплине.

4.1.4 Перечень информационных технологий и электронных ресурсов, используемых при осуществлении образовательного процесса по дисциплине (модулю)

Организовано взаимодействие обучающегося и преподавателя с использованием электронной информационно-образовательной среды КНИТУ-КАИ.

1. Сайт электронного обучения КНИТУ-КАИ http://e.kai.ru

4.1.5 Перечень ресурсов информационно-телекоммуникационной сети «Интернет», профессиональных баз данных, информационно-справочных систем, используемых при осуществлении образовательного процесса по дисциплине (модулю)

1 Электронно-библиотечная система учебной и научной литературы «Лань». URL: https://e.lanbook.com/.

2. Электронно-библиотечная система учебной и научной литературы «Znanium/com». URL: https://znanium.com/

3. Электронно-библиотечная система учебной и научной литературы «Юрайт». URL: https://urait.ru/catalog/full

4. Научно-техническая библиотека КНИТУ-КАИ им. Н.Г. Четаева. URL: http://elibs.kai.ru/

4.2 Материально-техническое обеспечение дисциплины (модуля) и требуемое программное обеспечение

Описание материально-технической базы и программного обеспечения, необходимого для осуществления образовательного процесса по дисциплине (модулю) приведено соответственно в таблицах 4.1 и 4.2.

Таблица 4.1

Материально-техническое обеспечение дисциплины (модуля)

Наименование вида учебных занятий	Наименование учебной аудитории, специализированной лаборатории	Перечень необходимого оборудования и технических средств обучения
Лекционные занятия	Учебная аудитория для проведения занятий лекционного типа ауд.№302	- мультимедийный проектор; - ноутбук; - настенный экран; - акустические колонки; - учебные столы, стулья; - доска; - стол преподавателя; - учебно – наглядные пособия.
Лабораторные занятия	Учебная аудитория для проведения практических занятий, текущего контроля и промежуточной аттестации (Компьютерная аудитория) ауд.№201	- компьютерные столы, стулья; - персональные компьютеры, ЖК мониторы; - доска интерактивная, - мультимедиа-проектор; - пакет операционных и прикладных программ.
Самостоятельная работа	Помещение для самостоятельной работы студента ауд.№112	- персональный компьютер (9 шт.); - ЖК монитор 19” (9 шт.); - столы компьютерные (9 шт.); - учебные столы (8 шт.), - стулья (25шт.).

Таблица 4.2

Лицензионное и свободно распространяемое программное обеспечение, в том числе отечественного производства, используемое при осуществлении образовательного процесса по дисциплине (модулю)

№ п/п	Наименование программного обеспечения	Производитель	Способ распространения (лицензионное или свободно распространяемое)
1.	Microsoft Windows 7 Professional Russian	Microsoft, США	Лицензионное
2.	Microsoft Office Professional Plus 2010 Russian	Microsoft, США	Лицензионное
3.	Антивирусная программа Kaspersky Endpoint Security 8 for Windows	Лаборатория Касперского, Россия	Лицензионное
4.	Microsoft Visual Studio	Microsoft, США	Лицензионное
5.	Matlab	The MathWorks	Лицензионное
6.	Microsoft Visio	Microsoft, США	Лицензионное
7.	Microsoft SQL Server	Microsoft, США	Свободно распространяемое
8.	XAMPP	Apachefriends.org	Свободно распространяемое
9.	PyCharm	JetBrains	Свободно распространяемое
10.	CISCO Packet Tracer	CISCO Systems	Свободно распространяемое

5 ОСОБЕННОСТИ РЕАЛИЗАЦИИ ДИСЦИПЛИНЫ (МОДУЛЯ) ДЛЯ ЛИЦ С ОГРАНИЧЕННЫМИ ВОЗМОЖНОСТЯМИ ЗДОРОВЬЯ И ИНВАЛИДОВ

Обучение по дисциплине (модулю) обучающихся с ограниченными возможностями здоровья и инвалидов осуществляется с учетом особенностей психофизического развития, индивидуальных возможностей и состояния здоровья таких обучающихся.

Обучение лиц с ограниченными возможностями здоровья и инвалидов организуется как совместно с другими обучающимися, так и в отдельных группах.

Для лиц с ограниченными возможностями здоровья и инвалидов предусмотрены дополнительные оценочные материалы, перечень которых указан в таблице 5.1.

Таблица 5.1

Дополнительные материалы оценивания для лиц с ограниченными возможностями здоровья и инвалидов

Категории обучающихся	Виды дополнительных оценочных материалов	Формы контроля и оценки результатов обучения
С нарушениями слуха	Тесты, контрольные работы, письменные самостоятельные работы, вопросы к (экзамену)	Преимущественно письменная проверка
С нарушениями зрения	Устный опрос по терминам, собеседование по вопросам к (экзамену)	Преимущественно устная проверка (индивидуально)
С нарушениями опорно-двигательного аппарата	Решение дистанционных тестов, контрольные работы, письменные самостоятельные работы, вопросы к (экзамену)	Преимущественно дистанционными методами

Для лиц с ограниченными возможностями здоровья и инвалидов предусматривается доступная форма предоставления заданий оценочных средств, например:

– в печатной форме;

– в печатной форме с увеличенным шрифтом;

– в форме электронного документа;

– методом чтения ассистентом задания вслух.

Лицам с ограниченными возможностями здоровья и инвалидам увеличивается время на подготовку ответов на контрольные вопросы. Для таких обучающихся предусматривается доступная форма предоставления ответов на задания, а именно:

– письменно на бумаге;

– набор ответов на компьютере;

– набор ответов с использованием услуг ассистента;

– представление ответов устно.

При необходимости для лиц с ограниченными возможностями здоровья и инвалидов процедура оценивания результатов обучения может проводиться в несколько этапов.

Учебно-методические материалы для самостоятельной и аудиторной работы обучающихся из числа лиц с ограниченными возможностями здоровья и инвалидов предоставляются в формах, адаптированных к ограничениям их здоровья и восприятия информации.

Освоение дисциплины (модуля) лицами с ограниченными возможностями здоровья и инвалидами осуществляется с использованием средств обучения общего и специального назначения.

ЛИСТ РЕГИСТРАЦИИ ИЗМЕНЕНИЙ

Изменения, вносимые в рабочую программу дисциплины (модуля)

№ п/п	№ раздела внесения изменений	Дата внесения изменений	Содержание изменений	«Согласовано» заведующий кафедрой, реализующей дисциплину