МИНОБРНАУКИ РОССИИ
Федеральное государственное бюджетное образовательное учреждение высшего образования
«САРАТОВСКИЙ НАЦИОНАЛЬНЫЙ ИССЛЕДОВАТЕЛЬСКИЙ ГОСУДАРСТВЕННЫЙ УНИВЕРСИТЕТ ИМЕНИ Н.Г. ЧЕРНЫШЕВСКОГО»
Факультет компьютерных наук и информационных технологий

УТВЕРЖДАЮ
Декан факультета
Миронов С. В.

«31» августа 2021 г.

Рабочая программа дисциплины
Методы и средства криптографической защиты информации

Специальность
10.05.01 Компьютерная безопасность

Специализация
Математические методы защиты информации

Квалификация выпускника
Специалист по защите информации

Форма обучения
Очная

Саратов,
2021

Статус	ФИО	Подпись	Дата
Преподаватель-разработчик	Жаркова А. В.		31.08.2021 г.
Председатель НМК	Кондратова Ю. Н.		31.08.2021 г.
Заведующий кафедрой	Абросимов М. Б.		31.08.2021 г.
Специалист Учебного управления	Юшинова И.В.		31.08.2021 г.

1. Цели освоения дисциплины

Целями освоения дисциплины являются овладение основными идеями и методами классической и современной криптографии; знакомство со средствами криптографической защиты информации; знание основополагающих документов в области защиты информации.

2. Место дисциплины в структуре ООП

Данная учебная дисциплина относится к обязательной части Блока 1 «Дисциплины (Модули)» учебного плана ООП и направлена на формирование у обучающихся общепрофессиональных компетенций.

Для изучения дисциплины необходимы компетенции, сформированные в результате изучения дисциплин «Алгебра», «Дискретная математика», «Теория вероятностей и математическая статистика», «Теория информации», «Математическая логика и теория алгоритмов», «Основы информационной безопасности»,

Компетенции, сформированные при изучении данной дисциплины, используются при изучении дисциплин «Криптографические протоколы», «Теоретико-числовые методы в криптографии», «Модели безопасности компьютерных систем», «Введение в криптоанализ», «Методы алгебраической геометрии в криптографии».

3. Результаты обучения по дисциплине

Код и наименование компетенции	Код и наименование индикатора (индикаторов) достижения компетенции	Результаты обучения
ОПК-10. Способен анализировать тенденции развития методов и средств криптографической защиты информации, использовать средства криптографической защиты информации при решении задач профессиональной деятельности.	ОПК-10.1.1 знает основные задачи, решаемые криптографическими методами; математические модели шифров, подходы к оценке их стойкости; зарубежные и российские криптографические стандарты; ОПК-10.2.1 умеет корректно использовать криптографические алгоритмы на практике при решении задач криптографическими методами; применять математические методы при исследовании криптографических алгоритмов; ОПК-10.3.1 владеет навыками использования типовых криптографических алгоритмов.	Знать основные задачи, решаемые криптографическими методами; математические модели шифров, подходы к оценке их стойкости; зарубежные и российские криптографические стандарты. Уметь корректно использовать криптографические алгоритмы на практике при решении задач криптографическими методами; применять математические методы при исследовании криптографических алгоритмов. Владеть навыками использования типовых криптографических алгоритмов.

Код и наименование компетенции	Код и наименование индикатора (индикаторов) достижения компетенции	Результаты обучения
ОПК-2.1. Способен разрабатывать алгоритмы, реализующие современные математические методы защиты информации.	ОПК-2.1.1 знает основные алгоритмы, реализующие современные математические методы защиты информации; ОПК-2.1.2 умеет применять алгоритмы, реализующие современные математические методы защиты информации; ОПК-2.1.3 владеет навыками разработки алгоритмов, реализующие современные математические методы защиты информации.	Знать основные алгоритмы, реализующие современные математические методы защиты информации. Уметь применять алгоритмы, реализующие современные математические методы защиты информации. Владеть навыками разработки алгоритмов, реализующие современные математические методы защиты информации.
ОПК-2.3. Способен проводить сравнительный анализ и осуществлять обоснованный выбор программных и программно-аппаратных средств защиты информации с учетом реализованных в них математических методов.	ОПК-2.3.1 знает основы проведения сравнительного анализа программных и программно-аппаратных средств защиты информации; ОПК-2.3.2 умеет проводить сравнительный анализ и осуществлять обоснованный выбор программных и программно-аппаратных средств защиты информации; ОПК-2.3.3 владеет навыками проведения сравнительного анализа и осуществления обоснованного выбора программных и программно-аппаратных средств защиты информации с учетом реализованных в них математических методов.	Знать основы проведения сравнительного анализа программных и программно-аппаратных средств защиты информации. Уметь проводить сравнительный анализ и осуществлять обоснованный выбор программных и программно-аппаратных средств защиты информации. Владеть навыками проведения сравнительного анализа и осуществления обоснованного выбора программных и программно-аппаратных средств защиты информации с учетом реализованных в них математических методов.

4. Структура и содержание дисциплины

Общая трудоемкость дисциплины составляет 8 зачетных единиц, 288 часов.

№ п/п	Раздел дисциплины	Семестр	Неделя семестра	Виды учебной работы, включая самостоятельную работу студентов и трудоемкость (в часах)					Формы текущего контроля успеваемости (по неделям семестра) Формы промежуточной аттестации (по семестрам)
				Лекции	Лабораторные занятия		ИКР	СР	
					Общая трудоёмкость	Из них – практическая подготовка			
1	2	3	4	5	6	7	8	9	10
	7-ой семестр								
1	Криптография, простейшие шифры	7	1–4	8	8	–	0,5	18	Опрос на 5-й неделе
2	Шифры многоалфавитной замены		5–8	8	8	–	0,5	18	
3	Надёжность шифров		9–13	9	9	–	0,5	19	*Контрольная работа* № 1 на 9-й неделе
4	Поточные шифрсистемы		13–17	9	9	–	0,5	19	Опрос на 14-й неделе
	Промежуточная аттестация								**Зачёт**
	ИТОГО в 7-м семестре – 144ч.			**34**	**34**	**–**	**2**	**74**	**–**
	8-ой семестр								
5	Блочные шифрсистемы	8	1–5	10	10	–	1	13	Опрос на 5-й неделе
6	Хэш-функции		6–11	11	11	–	1	13	*Контрольная работа* № 2 на 9-й неделе
7	Криптосистемы с открытым ключом		11–16	11	11	–	2	14	Опрос на 13-й неделе
	Промежуточная аттестация - 36								**Экзамен**
	ИТОГО в 8-м семестре – 144ч.			**32**	**32**	**–**	**4**	**40**	
	ВСЕГО			**288ч.**					

Содержание дисциплины

Криптография, простейшие шифры. Основные понятия. Алгебраические структуры. Открытые сообщения, характеристики, детерминированные и вероятностные модели открытых текстов. Критерии распознавания открытого текста. Математические модели шифров. Основные требования к шифрам. Шифры перестановки. Разновидности шифров перестановки: шифры горизонтальной перестановки, шифры вертикальной перестановки, маршрутные и геометрические перестановки. Элементы криптоанализа шифров перестановки. Шифры простой замены, лозунговые шифры. Использование частотных характеристик при анализе шифров простой замены и их усложнений.

Шифры многоалфавитной замены. Шифры многоалфавитной замены и гаммирования. Дисковые шифраторы, шифратор М-209, Enigma. Шифры гаммирования и их анализ.

Надёжность шифров. Энтропия языка. Расстояние единственности. Стойкость шифров, теоретическая и практическая стойкость. Имитостойкость шифров. Шифры, не распространяющие искажений.

Поточные шифрсистемы. Принципы построения. Линейные регистры сдвига. Усложнение линейной рекуррентной последовательности. Поточные шифрсистемы A5, RC4. Методы анализа поточных шифров.

Блочные шифрсистемы. Принципы построения. Структура алгоритмов, сеть Фейстеля, SP-сеть. S-блоки. Режимы шифрования. Методы анализа блочных шифрсистем. Блочные шифрсистемы DES, AES, ГОСТ Р 34.12–2015. ГОСТ Р 34.13–2015.

Хэш-функции. Основные свойства. Бесключевые и ключевые хэш-функции. Анализ хэш-функций. Современные криптографические хэш-функции и стандарты, MD5, SHA-1, стандарт ГОСТ 34.11–2012. Хэш-фунции на основе функции «губка», стандарт SHA-3.

Криптосистемы с открытым ключом. Вычислительно сложные задачи математики. Криптосистема RSA. Криптосистема Эль-Гамаля. Уравнение шифрования и формирования подписи. Связь с алгоритмами цифровой подписи. Криптосистемы Мак-Эллиса, Меркля-Хеллмана.

План лабораторных занятий

На лабораторных занятиях студенты знакомятся с основными сведениями, требуемыми для выполнения задания, выполняют лабораторные задания, в частности с использованием языков программирования C++, C#, Java, Python.

№ занятия	Тема	Задания для лабораторного практикума
1	**2**	**3**
1–4	Криптография, простейшие шифры	№ 1
5–8	Шифры многоалфавитной замены	№ 2
9–13	Надёжность шифров	№ 3
13–17	Поточные шифрсистемы	№ 4

№ занятия	Тема	Задания для лабораторного практикума
18–22	Блочные шифрсистемы	№ 5
23–28	Хэш-функции	№ 6
28–33	Криптосистемы с открытым ключом	№ 7

5. Образовательные технологии, применяемые при освоении дисциплины

Рекомендуемые образовательные технологии: встречи с представителями ведущих отечественных фирм по производству криптографической продукции, выступления экспертов и специалистов перед студентами, ознакомительные беседы с представителями потенциальных работодателей, экскурсия в музей регионального Управления ФСБ России, комментированное посещение Интернет-страницы музея криптологии Агентства национальной безопасности США в Форт-Миде.

Иная контактная работа представляет собой индивидуальные консультации, оказываемые очно и дистанционно с использованием информационных и телекоммуникационных технологий с учётом образовательных возможностей обучающихся.

При обучении лиц с ограниченными возможностями здоровья и инвалидов используются подходы, способствующие созданию безбарьерной образовательной среды: технологии дифференциации и индивидуализации обучения, сопровождение тьюторами в образовательном пространстве. При этом основной формой организации учебного процесса является интегрированное обучение лиц с ограниченными возможностями здоровья, т.е. все студенты обучаются в смешенных группах, имеют возможность постоянно общаться со сверстниками, благодаря чему легче адаптируются в социуме.

6. Учебно-методическое обеспечение самостоятельной работы студентов. Оценочные средства для текущего контроля успеваемости, промежуточной аттестации по итогам освоения дисциплины

В рамках самостоятельной работы студенты прорабатывают лекционный материал, изучают дополнительные сведения. Контроль текущей успеваемости осуществляется в процессе проведения лекционных и лабораторных занятий.

Фонд оценочных средств дисциплины включает в себя задания для самостоятельной работы, задания для лабораторных занятий, задания для контрольных работ, контрольные вопросы, вопросы для проведения промежуточной аттестации (зачёт), вопросы для проведения промежуточной аттестации (экзамен). Фонд оценочных средств оформлен в качестве приложения к учебной рабочей программе дисциплины «Методы и средства криптографической защиты информации».

7. Данные для учета успеваемости студентов в БАРС

Таблица 1.1 – Таблица максимальных баллов по видам учебной деятельности

1	2	3	4	5	6	7	8	9
Семестр	Лекции	Лабораторные занятия	Практические занятия	Самостоятельная работа	Автоматизированное тестирование	Другие виды учебной деятельности	Промежуточная аттестация	Итого
7	17	30	0	11	0	12	30	**100**
8	16	32	0	10	0	10	32	**100**

Программа оценивания учебной деятельности студента

7 семестр

Лекции

Посещаемость, опрос, активность и др. за один семестр – от 0 до 17 баллов.

Лабораторные занятия

Контроль выполнения лабораторных заданий, самостоятельность при выполнении работы, правильность выполнения, посещаемость в течение одного семестра – от 0 до 30 баллов.

Практические занятия

Не предусмотрены.

Самостоятельная работа

Контроль выполнения заданий в рамках самостоятельной работы, проверка усвоения изученного лекционного материала в рамках опроса, конспект занятий – от 0 до 11 баллов.

Автоматизированное тестирование

Не предусмотрено.

Другие виды учебной деятельности

Контроль выполнения *контрольной работы*, грамотность в оформлении, правильность выполнения – от 0 до 12 баллов.

Промежуточная аттестация

Промежуточная аттестация представляет собой теоретический *зачёт*, проводимый в виде собеседования в устной форме с предварительной подготовкой студента к ответу, или в письменном виде по выбору преподавателя.

При проведении промежуточной аттестации

ответ на «отлично» / «зачтено» оценивается от 24 до 30 баллов;

ответ на «хорошо» / «зачтено» оценивается от 19 до 23 баллов;

ответ на «удовлетворительно» / «зачтено» оценивается от 15 до 18 баллов;

ответ на «неудовлетворительно» / «не зачтено» оценивается от 0 до 14 баллов.

Таким образом, максимально возможная сумма баллов за все виды учебной деятельности студента за седьмой семестр по дисциплине «Методы и средства криптографической защиты информации» составляет **100** баллов.

Таблица 2.1 – Таблица пересчета полученной студентом суммы баллов по дисциплине «Методы и средства криптографической защиты информации» в оценку (зачёт)

70 баллов и более	«зачтено»
меньше 70 баллов	«не зачтено»

8 семестр

Лекции

Посещаемость, опрос, активность и др. за один семестр – от 0 до 16 баллов.

Лабораторные занятия

Контроль выполнения лабораторных заданий, самостоятельность при выполнении работы, правильность выполнения, посещаемость в течение одного семестра – от 0 до 32 баллов.

Практические занятия

Не предусмотрены.

Самостоятельная работа

Контроль выполнения заданий в рамках самостоятельной работы, проверка усвоения изученного лекционного материала в рамках опроса, конспект занятий – от 0 до 10 баллов.

Автоматизированное тестирование

Не предусмотрено.

Другие виды учебной деятельности

Контроль выполнения *контрольной работы*, грамотность в оформлении, правильность выполнения – от 0 до 10 баллов.

Промежуточная аттестация

Промежуточная аттестация представляет собой теоретический *экзамен*, проводимый в виде собеседования в устной форме с предварительной подготовкой студента к ответу, или в письменном виде по выбору преподавателя.

При проведении промежуточной аттестации

ответ на «отлично» оценивается от 26 до 32 баллов;

ответ на «хорошо» оценивается от 20 до 25 баллов;

ответ на «удовлетворительно» оценивается от 16 до 19 баллов;

ответ на «неудовлетворительно» оценивается от 0 до 15 баллов.

Таким образом, максимально возможная сумма баллов за все виды учебной деятельности студента за восьмой семестр по дисциплине «Методы и средства криптографической защиты информации» составляет **100** баллов.

Таблица 2.2 – Таблица пересчета полученной студентом суммы баллов по дисциплине «Методы и средства криптографической защиты информации» в оценку (экзамен)

80–100 баллов	«отлично»
64–79 баллов	«хорошо»
51–63 баллов	«удовлетворительно»
0–50 баллов	«неудовлетворительно»

8. Учебно-методическое и информационное обеспечение дисциплины

а) литература:

1) Основы криптографии [Текст] : учеб. пособие / А. П. Алфёров [и др.]. - 3-е изд., испр. и доп. - Москва : Гелиос АРВ, 2005. - 479, [1] с. - Библиогр.: с. 469-475. - ISBN 5-84438-137-0 (в пер.).

2) Салий, В. Н. Криптографические методы и средства защиты информации / В. Н. Салий. - Саратов : [б. и.], 2017. - 45 с. : ил. - URL: http://elibrary.sgu.ru/uch_lit/1851.pdf. - Библиогр.: с. 44-45 (15 назв.). - ~Б. ц.

3) Фомичёв, В. М. Криптографические методы защиты информации в 2 ч. Часть 1. Математические аспекты : Учебник для вузов / В. М. Фомичёв, Д. А. Мельников. - Москва : Юрайт, 2020. - 209 с. ISBN 978-5-9916-7088-3. URL: https://urait.ru/bcode/450820.

4) Фомичёв, В. М. Криптографические методы защиты информации в 2 ч. Часть 2. Системные и прикладные аспекты : Учебник для вузов / В. М. Фомичёв, Д. А. Мельников. - Москва : Юрайт, 2020. - 245 с. - (Высшее образование). - ISBN 978-5-9916-7090-6. URL: https://urait.ru/bcode/451486.

б) программное обеспечение и Интернет-ресурсы:

1) Лицензионное программное обеспечение: Visual C++ 4.2, Microsoft Visual Studio.

2) Свободное программное обеспечение: Java Developers Kit, NetBeans IDE, Eclipse, CPython, Jython, IronPython.

9. Материально-техническое обеспечение дисциплины

Для проведения лекционных занятий необходима лекционная аудитория, в которой имеются учебная доска, компьютер с возможностью выхода в сеть Интернет, мультимедийный проектор с экраном с возможностью демонстрации электронной презентации.

Для проведения лабораторных занятий необходим компьютерный класс, оснащенный соответствующим программным обеспечением, с возможностью выхода в сеть Интернет.

Программа составлена в соответствии с требованиями ФГОС ВО по специальности 10.05.01 Компьютерная безопасность, специализация «Математические методы защиты информации» (квалификация «Специалист по защите информации»).

Автор

Доцент кафедры теоретических основ компьютерной безопасности и криптографии, кандидат физико-математических наук А. В. Жаркова

Программа одобрена на заседании кафедры теоретических основ компьютерной безопасности и криптографии от «31» августа 2021 года, протокол № 1.