МИНИСТЕРСТВО НАУКИ И ВЫСШЕГО ОБРАЗОВАНИЯ
РОССИЙСКОЙ ФЕДЕРАЦИИ

Федеральное государственное бюджетное образовательное учреждение
высшего образования
«Магнитогорский государственный технический университет им. Г.И. Носова»

УТВЕРЖДАЮ
Директор ИЭиАС
С.И. Лукьянов

26.02.2020 г.

РАБОЧАЯ ПРОГРАММА ДИСЦИПЛИНЫ (МОДУЛЯ)

ТЕХНОЛОГИИ КРИПТОГРАФИЧЕСКОЙ ЗАЩИТЫ ДЛЯ ФИНАНСОВОЙ ИНДУСТРИИ

Направление подготовки (специальность)
09.04.01 Информатика и вычислительная техника

Направленность (профиль/специализация) программы
Программное обеспечение средств вычислительной техники и автоматизированных систем

Уровень высшего образования - магистратура

Форма обучения
очная

Институт/ факультет	Институт энергетики и автоматизированных систем
Кафедра	Вычислительной техники и программирования
Курс	2
Семестр	3

Магнитогорск
2020 год

Рабочая программа составлена на основе ФГОС ВО - магистратура по направлению подготовки 09.04.01 Информатика и вычислительная техника (приказ Минобрнауки России от 19.09.2017 г. № 918)

Рабочая программа рассмотрена и одобрена на заседании кафедры Вычислительной техники и программирования
19.02.2020 г. протокол № 5

Зав. кафедрой _____ О.С. Логунова

Рабочая программа одобрена методической комиссией ИЭ и АС
26.02.2020 г. протокол № 5

Председатель _____ С.И. Лукьянов

Рабочая программа составлена:
ООО "Компас Плюс" , _____ А.Е. Лубрик
зав. кафедрой ВТ и П, д-р техн. Наук _____ О.С. Логунова
доцент кафедры ВТ и П, канд. техн. наук _____ Ю.В. Кочержинская

Рецензент:
Начальник отдела технологических платформ
ООО "Компас Плюс" , канд. техн. наук _____ Д.С. Сафонов

Лист актуализации рабочей программы

Рабочая программа пересмотрена, обсуждена и одобрена для реализации в 2021 - 2022 учебном году на заседании кафедры Вычислительной техники и программирования

Протокол от __ _____ 20__ г. № __
Зав. кафедрой _____ О.С. Логунова

Рабочая программа пересмотрена, обсуждена и одобрена для реализации в 2022 - 2023 учебном году на заседании кафедры Вычислительной техники и программирования

Протокол от __ _____ 20__ г. № __
Зав. кафедрой _____ О.С. Логунова

1 Цели освоения дисциплины (модуля)

Дисциплина "Технологии криптографической защиты для финансовой индустрии" содержит основные положения криптографии, знакомит с наиболее распространенными типами шифров и методами их криптоанализа, понятиями целостности информации, криптографическими протоколами , электронной подписью. Объясняется математическая теория, лежащая в основе криптографии (теория групп, полей Галуа, неприводимые многочлены, теория чисел, псевдослучайные последовательности и др.). Ставятся вопросы реализации алгоритмов шифрования и криптоанализа.

2 Место дисциплины (модуля) в структуре образовательной программы

Дисциплина Технологии криптографической защиты для финансовой индустрии входит в часть учебного плана формируемую участниками образовательных отношений образовательной программы.

Для изучения дисциплины необходимы знания (умения, владения), сформированные в результате изучения дисциплин/ практик:

Программное обеспечение современной перспективной платежной инфраструктуры

Технология разработки программного обеспечения

Современные автоматизированные системы для платежей и розничных банковских процессов

Анализ и описание профессиональной информации

Знания (умения, владения), полученные при изучении данной дисциплины будут необходимы для изучения дисциплин/практик:

Выполнение и защита выпускной квалификационной работы

3 Компетенции обучающегося, формируемые в результате освоения дисциплины (модуля) и планируемые результаты обучения

В результате освоения дисциплины (модуля) «Технологии криптографической защиты для финансовой индустрии» обучающийся должен обладать следующими компетенциями:

Код индикатора	Индикатор достижения компетенции
ПК-4 Обладает способностью к разработке компонентов системы управления базами данных, отладке разрабатываемой системы управления базами данных, документированию разработанной системы управления базами данных в целом и ее компонентов и сопровождению созданной системы управления базами данных	
ПК-4.1	Определяет необходимость разработки компонентов системы управления базами данных
ПК-4.2	Оценивает качество разработки компонентов системы управления базами данных

4. Структура, объём и содержание дисциплины (модуля)

Общая трудоемкость дисциплины составляет 4 зачетных единиц 144 акад. часов, в том числе:

– контактная работа – 34,1 акад. часов:

– аудиторная – 34 акад. часов;

– внеаудиторная – 0,1 акад. часов

– самостоятельная работа – 109,9 акад. часов;

Форма аттестации - зачет с оценкой

Раздел/ тема дисциплины	Семестр	Аудиторная контактная работа (в акад. часах)			Самостоятельная работа студента	Вид самостоятельной работы	Форма текущего контроля успеваемости и промежуточной аттестации	Код компетенции
		Лек.	лаб. зан.	практ. зан.				
1. Основы криптографии								
1.1 Основные задачи криптосистемы. Симметричные криптосистемы. Блочные и поточные шифры. Алгоритм 3DES. Криптография с открытым ключом. Криптографические хэш-функции	3		6/6И		20	Повторение основных вопросов по дисциплине "Защита информации". Подготовка к выполнению лабораторной работе.	Дискуссия. Проверка выполнения лабораторной работы.	ПК-4.1, ПК-4.2
1.2 Форматы PIN-блока. Методы проверки PIN. Методы проверки карты. Аутентификация сообщений			7/7И		15	Повторение основных вопросов по дисциплине "Защита информации". Подготовка к выполнению лабораторной работе.	Дискуссия. Проверка выполнения лабораторной работы.	ПК-4.1, ПК-4.2
1.3 Криптографические ключи: иерархия ключей; ключи терминалов; ключи карточных префиксов; хостовые			7/3И		15	Подготовка к выполнению лабораторной работе.	Дискуссия. Проверка выполнения лабораторной работы.	ПК-4.1, ПК-4.2
Итого по разделу			20/16И		50			
2. Криптография процессинговой системы								
2.1 Настройка модуля процессинговой системы: поддерживаемое оборудование; модуль «Криптосервер»; настройка системы	3		7		12,9	Подготовка к выполнению лабораторной работе.	Дискуссия. Проверка выполнения лабораторной работы.	ПК-4.1, ПК-4.2

2.2 Система учета и генерации криптоключей: основные функции; статусы ключей; список ответственных лиц; шаблоны печати открытых компонент; задачи пакетной генерации ключей; пакетные процедуры;			7		7	Подготовка к выполнению лабораторной работе.	Дискуссия. Проверка выполнения лабораторной работы.	ПК-4.1, ПК-4.2
Итого по разделу			14		19,9			
3. Зачет								
3.1 Зачет	3				40	Подготовка к зачету	Зачет с оценкой	ПК-4.1, ПК-4.2
Итого по разделу					40			
Итого за семестр			34/16И		109,9		зао	
Итого по дисциплине			34/16И		109,9		зачет с оценкой	

5 Образовательные технологии

1. Традиционные образовательные технологии, ориентированные на организацию образовательного процесса и предполагающую прямую трансляцию знаний от преподавателя к студенту.

Формы учебных занятий с использованием традиционных технологий:

Информационная лекция – последовательное изложение материала в дисциплинарной логике, осуществляемое преимущественно вербальными средствами (монолог преподавателя).

Лабораторная работа – организация учебной работы с реальными материальными и информационными объектами, экспериментальная работа с аналоговыми моделями реальных объектов.

2. Технологии проблемного обучения – организация образовательного процесса, которая предполагает постановку проблемных вопросов, создание учебных проблемных ситуаций для стимулирования активной познавательной деятельности студентов.

3. Интерактивные технологии – организация образовательного процесса, которая предполагает активное и нелинейное взаимодействие всех участников, достижение на этой основе личностно значимого для них образовательного результата.

Формы учебных занятий с использованием специализированных интерактивных технологий:

Лекция «обратной связи» – лекция–провокация (изложение материала с заранее запланированными ошибками), лекция-беседа, лекция-дискуссия, лекция-конференция.

4. Информационно-коммуникационные образовательные технологии – организация образовательного процесса, основанная на применении программных сред и технических средств работы со знаниями в различных предметных областях.

6 Учебно-методическое обеспечение самостоятельной работы обучающихся

Представлено в приложении 1.

7 Оценочные средства для проведения промежуточной аттестации

Представлены в приложении 2.

8 Учебно-методическое и информационное обеспечение дисциплины (модуля)

а) Основная литература:

1.Жук А. П. Защита информации: Учебное пособие / А.П. Жук, Е.П. Жук, О.М. Лепешкин, А.И. Тимошкин. - 2-е изд. - М.: ИЦ РИОР: НИЦ ИНФРА-М, 2015. - 392 с. Режим доступа: http://znanium.com/bookread.php?book=474838 Электронный ресурс

2.Бабаш А. В. Криптографические методы защиты информации. Учебно-методическое пособие / А.В. Бабаш. - 2-е изд. - М.: ИЦ РИОР: НИЦ ИНФРА-М, 2014. - 216 с. Режим доступа: http://znanium.com/bookread.php?book=432654 Электронный ресурс

3.Баранова Е. К. Моделирование системы защиты информации: Практикум: Учебное пособие / Е.К.Баранова, А.В.Бабаш - М.: ИЦ РИОР: НИЦ ИНФРА-М, 2015 - 120 с. Режим доступа: http://znanium.com/bookread.php?book=476047 Электронный ресурс

б) Дополнительная литература:

1. Техническая документация открытой технологической платформы TranzAxis.

2. https://compassplus.ru/static/materials/leaflets/TranzAxis_Differentiators_Leaflet.pdf

в) Методические указания:

Глоссарий по криптографии - https://hpc.name/text/get/82/p1.html
литературапо криптографии - http://www.proklondike.com/books/crypto.html
сайт лаборатории радиосистем (кафедра радиофизики) - http://radiosys.ksu.ru
Сайт по криптографии - http://kek.ksu.ru/Student/Crypto/Main.htm
электронные книги по криптографии - http://www.knigka.info/kriptograf/

г) Программное обеспечение и Интернет-ресурсы:

Программное обеспечение

Наименование ПО	№ договора	Срок действия лицензии
MS Windows 7 Professional(для классов)	Д-1227-18 от 08.10.2018	11.10.2021
FlowVision	К-93-09 от 19.06.2009	бессрочно
Borland Turbo C++	№112301 от 23.11.2005	бессрочно
Eclipse	свободно распространяемое ПО	бессрочно

Профессиональные базы данных и информационные справочные системы

Название курса	Ссылка
Национальная информационно-аналитическая система – Российский индекс научного цитирования (РИНЦ)	URL: https://elibrary.ru/project_risc.asp
Поисковая система Академия Google (Google Scholar)	URL: https://scholar.google.ru/
Федеральное государственное бюджетное учреждение «Федеральный институт промышленной собственности»	URL: http://www1.fips.ru/

9 Материально-техническое обеспечение дисциплины (модуля)

Материально-техническое обеспечение дисциплины включает:

1. Лекционная аудитория Мультимедийные средства хранения, передачи и представления информации

2. Компьютерный класс. Персональные компьютеры с виртуальной машиной для установки серверного ПО, выходом в Интернет и с доступом в электронную информационно-образовательную среду университета.

3. Аудитории для самостоятельной работы: компьютерные классы; читальные залы библиотеки. Все классы УИТ и АСУ с персональными компьютерами, выходом в Интернет и с доступом в электронную информационно-образовательную среду университета.

4. Аудиторий для групповых и индивидуальных консультаций, текущего контроля и промежуточной аттестации. Ауд. 282 и классы УИТ и АСУ.

5. Помещения для самостоятельной работы обучающихся, оснащенных компьютерной техникой с возможностью подключения к сети «Интернет» и наличием доступа в электронную информационно-образовательную среду организации. Классы УИТ и АСУ.

6. Помещения для хранения и профилактического обслуживания учебного оборудования. Центр информационных технологий – ауд. 372

Приложение 1
«Учебно-методическое обеспечение самостоятельной работы обучающихся»

Глоссарий по криптографии - https://hpc.name/text/get/82/p1.html
литературапо криптографии - http://www.proklondike.com/books/crypto.html
сайт лаборатории радиосистем (кафедра радиофизики) - http://radiosys.ksu.ru
Сайт по криптографии - http://kek.ksu.ru/Student/Crypto/Main.htm
электронные книги по криптографии - http://www.knigka.info/kriptograf/

Приложение 2

7 Оценочные средства для проведения промежуточной аттестации

а) Планируемые результаты обучения и оценочные средства для проведения промежуточной аттестации:

<table>
<tr><th>Код индикатора</th><th>Индикатор достижения компетенции</th><th>Оценочные средства</th></tr>
<tr><td colspan="3">ПК-4: Обладает способностью к разработке компонентов системы управления базами данных, отладке разрабатываемой системы управления базами данных, документированию разработанной системы управления базами данных в целом и ее компонентов и сопровождению созданной системы управления базами данных</td></tr>
<tr><td>ОПК-4.1</td><td>Определяет необходимость разработки компонентов системы управления базами данных</td><td rowspan="2">Перечень теоретических вопросов
1. Основные задачи криптосистемы. Симметричные криптосистемы. Блочные и поточные шифры. Алгоритм 3DES. Криптография с открытым ключом. Криптографические хэш-функции.
2. Форматы PIN-блока. Методы проверки PIN. Методы проверки карты. Аутентификация сообщений.
3. Криптографические ключи: иерархия ключей; ключи терминалов; ключи карточных префиксов; хостовые ключи.
4. Настройка модуля процессинговой системы: поддерживаемое оборудование; модуль «Криптосервер»; настройка системы.
5. Система учета и генерации криптоключей: основные функции; статусы ключей; список ответственных лиц; шаблоны печати открытых компонент; задачи пакетной генерации ключей; пакетные процедуры; операции с ключами.</td></tr>
<tr><td>ОПК-4.2</td><td>Оценивает качество разработки компонентов системы управления базами данных</td></tr>
</table>

б) Порядок проведения промежуточной аттестации, показатели и критерии оценивания:

Промежуточная аттестация по дисциплине включает теоретические вопросы, позволяющие оценить уровень усвоения обучающимися знаний, и практические задания, выявляющие степень сформированности умений и владений, проводится в форме в форме зачета с оценкой.

Зачет с оценкой по дисциплине проводится в устной форме по экзаменационным билетам, каждый из которых включает два теоретических вопроса и одно практическое задание.

Показатели и критерии оценивания зачета с оценкой:

– на оценку **«отлично»** (5 баллов) – обучающийся демонстрирует высокий уровень сформированности компетенций, всестороннее, систематическое и глубокое знание учебного материала, свободно выполняет практические задания, свободно оперирует знаниями, умениями, применяет их в ситуациях повышенной сложности.

– на оценку **«хорошо»** (4 балла) – обучающийся демонстрирует средний уровень сформированности компетенций: основные знания, умения освоены, но допускаются незначительные ошибки, неточности, затруднения при аналитических операциях, переносе знаний и умений на новые, нестандартные ситуации.

– на оценку **«удовлетворительно»** (3 балла) – обучающийся демонстрирует пороговый уровень сформированности компетенций: в ходе контрольных мероприятий допускаются ошибки, проявляется отсутствие отдельных знаний, умений, навыков, обучающийся испытывает значительные затруднения при оперировании знаниями и умениями при их переносе на новые ситуации.

– на оценку **«неудовлетворительно»** (2 балла) – обучающийся демонстрирует знания не более 20% теоретического материала, допускает существенные ошибки, не может показать интеллектуальные навыки решения простых задач.

– на оценку **«неудовлетворительно»** (1 балл) – обучающийся не может показать знания на уровне воспроизведения и объяснения информации, не может показать интеллектуальные навыки решения простых задач.

1. Основные понятия, термины, определения. Криптология, криптография, криптоанализ, аутентификация, идентификация. Основные причины использования криптосистем. Симметричная криптосистема. 2. Исторические шифры. Шифр сдвига. Шифр замены. Полиалфавитный шифр. Шифр Виженера. Шифр Вернама. Недостатки исторических шифров. (Информационная стойкость). 3. Информационная стойкость криптографических систем Вычислительно защищенная криптосистема. Основные проблемы вычислительно защищенной криптосистемы. Абсолютно стойкая (совершенная) криптосистема. 4. К какому классу криптосистем - вычислительно защищенной или абсолютно стойкой относятся следующие криптосистемы: Шифр сдвига. Шифр замены. Шифр Виженера. Шифр Вернама ? 5. Понятие "абсолютной стойкости" в терминах теории вероятности. Теорема Шеннона: критерий абсолютной стойкости шифра. Интерпретация на примере шифра Вернама. Программа дисциплины "Криптографические методы защиты информации"; 090900.62 Информационная безопасность; профессор, д.н. (профессор) Карпов А.В. Регистрационный номер 6170314 Страница 8 из 11. 6. Энтропия случайной величины. Свойства энтропии. совместная энтропия двух случайных величин. Условная энтропия двух случайных величин. Неопределенность ключа. 7. Энтропия естественного языка. Расстояние единственности шифра. 8. Криптосистема с секретным ключом. Принцип Керкхоффа. Поточные и блочные шифры. 9. Поточные шифры. Генератор ключевого потока. Свойства генератора ключевого потока. Генератор псевдослучайных чисел, основанный на использовании алгебраических свойств М-последовательностей 10. Статистические тесты генераторов ключевого потока. 11. Блочные шифры. Алгоритм

DES. Перестановки. Раунды. Алгоритм Фейстеля при шифровании и дешифровании. 12. Сравнение блочных и поточных шифров. Методы организации процедуры исправления ошибок. 13. Статичный ключ. Эфемерный ключ. Распределение ключей. Основные пути решения проблемы распределения ключей. (физические методы, Протоколы с секретным ключом, Протоколы с открытым ключом, современные физические методы). 14. Разделение секрета. Схема порогового разделения секрета. (T, W) - пороговая схема Шамира. 15. Протоколы распределения секретных ключей. Основные цели протокола распределения ключей. Протокол Барроуза. 16. Протоколы распределения секретных ключей. Основные цели протокола распределения ключей. Протокол Нидхейма-Шредера 17. Протоколы распределения секретных ключей. Основные цели протокола распределения ключей. Протокол Отвэй-Риса. 18. Протоколы распределения секретных ключей. Основные цели протокола распределения ключей. Цербер 19. Арифметика остатков. Сравнение по модулю. Решение уравнения ax = b (mod N). 20. Функция Эйлера. Мультипликативные обратные по модулю N. Теорема Лагранжа. Малая теорема Ферма. Применение в криптографии. 21. Алгоритм Евклида. Китайская теорема об остатках. Расширенный алгоритм Евклида. Применение в криптографии. 22. Криптосистема с открытым ключом. Криптографическая односторонняя функция. Важнейшие криптографические односторонние функции. 23. Оценка сложности задач. Сложность алгоритма: Полиноминальная, экспоненциальная, субэкспоненциальная Оракул. Сравнительный анализ сложности криптографических алгоритмов (без доказательства). 24. Алгоритм RSA. Шифрование в RSA. Дешифрование в RSA. Доказательство алгоритма. 25. Алгоритм RSA. Задача криптоаналитика. Криптостойкость RSA 26. Криптосистема Эль-Гамаль. Параметры домена. Шифрование. Дешифрование. 27. Криптосистема Рабина. Алгоритм. Шифрование. Дешифрование. 28. Простые числа. Важность проблемы тестирования простых чисел. Пробное деление. Вероятностный подход при определении простого числа. Тест Ферма. Тест Миллера ? Рабина. 29. Распределение ключей Диффи ? Хеллмана. Алгоритм. Стойкость. Атака человек посередине. Необходимость использования цифровой подписи. 30. Алгоритмом цифровой подписи RSA 31. Криптографическая Хэш-функция. Свойства криптографической хэш-функции.Свойство односторонности Защищенность от повторений, защищенностью от вторых прообразов. 32. Алгоритмом цифровой подписи DSA 33. Отечественный стандарт цифровой подписи ГОСТ Р 34.10-94 34. Квантовая криптография 35. Передача секретных ключей по радиоканалу