МИНИСТЕРСТВО НАУКИ И ВЫСШЕГО ОБРАЗОВАНИЯ РОССИЙСКОЙ ФЕДЕРАЦИИ

ФЕДЕРАЛЬНОЕ ГОСУДАРСТВЕННОЕ БЮДЖЕТНОЕ ОБРАЗОВАТЕЛЬНОЕ УЧРЕЖДЕНИЕ ВЫСШЕГО ОБРАЗОВАНИЯ «ГРОЗНЕНСКИЙ ГОСУДАРСТВЕННЫЙ НЕФТЯНОЙ ТЕХНИЧЕСКИЙ УНИВЕРСИТЕТ ИМЕНИ АКАДЕМИКА М.Д.МИЛЛИОНЩИКОВА»

«Информационные системы в экономике»
(наименование кафедры)

УТВЕРЖДЕН

на заседании кафедры
«_02_» ___09__2023г., протокол № 1

Заведующий кафедрой
_____ Л.Р.Магомаева
(подпись)

ФОНД ОЦЕНОЧНЫХ СРЕДСТВ ПО УЧЕБНОЙ ДИСЦИПЛИНЕ

«Информационная безопасность в цифровой экономике»
(наименование дисциплины)

Направление подготовки
38.04.05 «Бизнес- информатика»
(код и наименование направления/ специальности подготовки)

Профиль подготовки
«Электронный бизнес»
(наименование специализации / профиля подготовки)

Квалификация
_____магистр_____
(специалист / бакалавр / магистр)

Год начала подготовки: 2021

Составитель (и) _____ М.К. Абдулаев
(подпись)

Грозный – 2023

ПАСПОРТ

ФОНДА ОЦЕНОЧНЫХ СРЕДСТВ ПО УЧЕБНОЙ ДИСЦИПЛИНЕ

«Информационная безопасность в цифровой экономике»

(наименование дисциплины)

№ п/п	Контролируемые разделы (темы) дисциплины	Код контролируемой компетенции (или ее части)	Наименование оценочного средства
1.	**Раздел 1**. Анализ рисков в области защиты информации	ПК-5	Лабораторная работа
2.	**Раздел 2.** Технологии анализа рисков	ПК-5	Лабораторная работа
3.	**Раздел 3.** Аудит безопасности и анализ рисков	ПК-5	Лабораторная работа
4.	**Раздел 4.** Обнаружение атак и управление рисками	ПК-5	Лабораторная работа

ПРИМЕРНЫЙ ПЕРЕЧЕНЬ ОЦЕНОЧНЫХ СРЕДСТВ

№ п/п	Наименование оценочного средства	Краткая характеристика оценочного средства	Представление оценочного средства в фонде
1.	*Лабораторная работа*	Средство проверки умений применять полученные знания по заранее определенной методике для решения задач или заданий по модулю или дисциплине в целом	Задания для выполнения лабораторных работ
2	*Рубежный контроль*	Форма проверки знаний по дисциплине в виде первой и второй рубежных аттестаций	-
3	*Зачет*	Итоговая форма оценки знаний	Вопросы к зачету

ЗАДАНИЯ ДЛЯ ВЫПОЛНЕНИЯ ЛАБОРАТОРНЫХ РАБОТ

Лабораторная работа №1 (ПК-5)

Использование библиотек длинночисленных типов данных для реализации криптографических преобразований

Лабораторная работа №2

Программная реализация компонентов блочного шифра «Магма» ГОСТ Р 34.12-2015.

Лабораторная работа №3(ПК-5)

Программная реализация компонентов блочного шифра «КУЗНЕЧИК» ГОСТ Р 34.12-2015

Лабораторная работа №4

Программная реализация режимов шифрования по ГОСТ Р 34.13-2015

Лабораторная работа №5 (ПК-5)

Программная реализация компонентов функции хеширования «Стрибог» ГОСТ Р 34.11-2012

Лабораторная работа №6

Построение криптографических протоколов с использованием ruToken CSP

Критерии оценки ответов на лабораторные работы:

- **не зачтено выставляется магистранту**, если дан неполный ответ, представляющий собой разрозненные знания по теме вопроса с существенными ошибками в определениях. Присутствуют фрагментарность, нелогичность изложения. магистрант не осознает связь данного понятия, теории, явления с другими объектами дисциплины. Отсутствуют выводы, конкретизация и доказательность изложения. Речь неграмотная. Дополнительные и уточняющие вопросы преподавателя не приводят к коррекции ответа студента не только на поставленный вопрос, но и на другие вопросы дисциплины.

- **зачтено выставляется магистранту**, если дан полный, развернутый ответ на поставленный вопрос, показана совокупность осознанных знаний об объекте, доказательно раскрыты основные положения темы; в ответе прослеживается четкая структура, логическая последовательность, отражающая сущность раскрываемых понятий, теорий, явлений. Знание об объекте демонстрируется на фоне понимания его в системе данной науки и междисциплинарных связей. Ответ изложен литературным языком в терминах науки. Могут быть допущены недочеты в определении понятий, исправленные магистрантом самостоятельно в процессе ответа.

ГРОЗНЕНСКИЙ ГОСУДАРСТВЕННЫЙ НЕФТЯНОЙ ТЕХНИЧЕСКИЙ УНИВЕРСИТЕТ ИМЕНИ АКАДЕМИКА М.Д.МИЛЛИОНЩИКОВА

Институт цифровой экономики и технологического предпринимательства
Кафедра информационные системы в экономике

Вопросы итогового контроля по дисциплине «Информационная безопасность в цифровой экономике»

Вопросы к зачету

1. Базовый (Baseline) анализ рисков. (ПК-5)
2. Полный (Full) анализ рисков
3. Угроза ИБ
4. Источник угрозы (ПК-5)
5. Последствия атаки
6. Несанкционированный доступ к данным через скрытые элементы данных.
7. Неправильное хранение носителей информации в случае аварий.
8. Риск нарушения ИБ (ПК-5)
9. Анализ уязвимости
10. Недостатки в документировании коммуникаций.
11. Разрушение оборудования или данных в результате небрежности.
12. Опасности, связанные с увольнением или выведением персонала за штат.
13. Запрещенные действия в информационной системе. (ПК-5)
14. Запрещенные действия системного администратора.
15. Неправильное администрирование сайта и прав доступа.
16. Смена пользователей ПК, не соответствующая внутренним правилам
17. Нарушение правил администрирования DBMS
18. Небрежность манипуляций с данными
19. Недостатки системы сегментации.
20. Уязвимости ПО или ошибки.

Критерии оценки ответов на зачете:

Оценка **«зачтено»** выставляется магистранту, сформулировавшему достаточно полные и правильны е ответы на поставленные вопросы. При ответе студент продемонстрировал владение основными терминами, логически верно и аргументировано выстраивал свой ответ, знал содержание учебной и научной литературы. Студент также правильно ответил на уточняющие и дополнительные вопросы.

Оценка **«не зачтено»** выставляется магистранту, если он не дал ответа хотя бы по одному вопросу билета, либо дал неверные, содержащие фактические ошибки ответы на все вопросы, не смог ответить на дополнительные и уточняющие вопросы. Оценка **«незачет»** ставится магистранту, отказавшемуся отвечать по билету или не явившемуся на зачёт.

Приложение 1

КОМПЛЕКТ ЗАДАНИЙ ДЛЯ ВЫПОЛНЕНИЯ ЛАБОРАТОРНЫХ РАБОТ

Лабораторная работа 1.

Использование библиотек длинночисленных типов данных для реализации криптографических преобразований

Целью работы является изучение следующих элементов программно-аппаратной реализации криптографических протоколов:

- изучение программной реализации длинночисленной арифметики на примере класса BigInteger C#.
- программная реализация базовых теоретико-числовых и криптографических алгоритмов.

1. ПОРЯДОК ВЫПОЛНЕНИЯ РАБОТЫ

Лабораторная работа проводится в виде семинара с последующим выполнением программной реализации компонентов криптографического протокола. Тематика семинара соответствует теме лабораторной работы. Для подготовки следует использовать соответствующую литературу и источники сети Интернет. После обсуждения каждому студенту в соответствии с индивидуальным заданием предлагается реализовать одно или несколько базовых преобразований алгоритма в среде программирования MS Visual Studio (конфигурация C#).

2. КОНТРОЛЬНЫЕ ЗАДАНИЯ

1. Перечислите основные способы хранения больших чисел.
2. В чем отличие процедур сложения и вычитания больших чисел?
3. Опишите основную идею цмножения больших чисел «в столбик».
4. Опишите «наивное» модульное экспоненцирование.
5. Опишите бинарный алгоритм модульного экспоненцирования.
6. Какова особенность использования знаковых типов данных при реализации расширенного алгоритма Евклида?
7. Какова основная идея теста Ферма?
8. В чем заключаются недостатки теста Ферма?
9. Какове число повторений теста Миллера-Рабина выполняется на практике при проверке числа на простоту?

Лабораторная работа 2.

Программная реализация компонентов блочного шифра «Магма» ГОСТ Р 34.12-2015

1. ЦЕЛЬ РАБОТЫ

Целью работы является изучение следующих элементов криптографических протоколов и стандартов:

- термины и определения.
- математический аппарат.
- базовые криптографические преобразования.
- программная реализация.

2. ПОРЯДОК ВЫПОЛНЕНИЯ РАБОТЫ

Лабораторная работа проводится в виде семинара с последующим выполнением программной реализации компонентов криптографического стандарта. Тематика семинара соответствует теме лабораторной работы. Для подготовки следует использовать соответствующую литературу и источники сети Интернет. После обсуждения каждому студенту в соответствии с индивидуальным заданием предлагается реализовать одно или несколько базовых преобразований алгоритма в произвольной среде программирования. Для проверки правильности реализации используются контрольные примеры, приведенные в методических указаниях и ГОСТ Р 34.12-2015.

3. КОНТРОЛЬНЫЕ ЗАДАНИЯ

1. Почему функция f раунда сети Файстеля может быть необратимой?
2. Поясните смысл финальной перестановки подблоков в последнем раунде сети Файстеля.
3. В чем отличие процедур зашифрования и расшифрования?
4. В каком случае процедуры зашифрования и расшифрования совпадают?
5. Перечислите основные характеристики алгоритма блочного шифрования «Магма» ГОСТ Р 34.12-2015.
6. Назовите основные требования к подстановкам.
7. Какие типы данных использовались в программной реализации?
8. Какими способами можно программно реализовать циклический битовый сдвиг?
9. Охарактеризуйте особенности программной реализации битовых подстановок?

Лабораторная работа 3.

Программная реализация компонентов блочного шифра «КУЗНЕЧИК» ГОСТ Р 34.12-2015

1. ЦЕЛЬ РАБОТЫ

Целью работы является изучение следующих элементов криптографических протоколов и стандартов:

- термины и определения.
- математический аппарат.
- базовые криптографические преобразования.
- программная реализация.

2. ПОРЯДОК ВЫПОЛНЕНИЯ РАБОТЫ

Лабораторная работа проводится в виде семинара с последующим выполнением программной реализации компонентов криптографического стандарта. Тематика семинара соответствует теме лабораторной работы. Для подготовки следует использовать соответствующую литературу и источники сети Интернет. После обсуждения каждому студенту в соответствии с индивидуальным заданием предлагается реализовать одно или несколько базовых преобразований алгоритма в произвольной среде программирования. Для проверки правильности реализации используются контрольные примеры, приведенные в методических указаниях и ГОСТ Р 34.12-2015.

3. КОНТРОЛЬНЫЕ ЗАДАНИЯ

1. Перечислите основные характеристики алгоритма блочного шифрования «Кузнечик» ГОСТ Р 34.12-2015.
2. Какую базовую структуру использует алгоритм «Кузнечик»?
3. Охарактеризуйте раундовую функцию алгоритма.
4. В чем отличие процедур зашифрования и расшифрования?
5. Какая базовая структура используется при развертывании подключей?
6. В чем отличие *S*-подстановок алгоритмов «Магма» и «Кузнечик».

7. Какие типы данных использовались в программной реализации?
8. Охарактеризуйте отличия программных реализаций алгоритмов «Магма» и «Кузнечик».
9. Охарактеризуйте особенности программной реализации линейного преобразования?

Лабораторная работа 4.

Программная реализация режимов шифрования по ГОСТ Р 34.13-2015

1. ЦЕЛЬ РАБОТЫ

Целью работы является изучение следующих элементов криптографических протоколов и стандартов:

- термины и определения.
- математический аппарат.
- базовые криптографические преобразования.
- программная реализация.

2. ПОРЯДОК ВЫПОЛНЕНИЯ РАБОТЫ

Лабораторная работа проводится в виде семинара с последующим выполнением программной реализации компонентов криптографического стандарта. Тематика семинара соответствует теме лабораторной работы. Для подготовки следует использовать соответствующую литературу и источники сети Интернет. После обсуждения каждому студенту в соответствии с индивидуальным заданием предлагается реализовать одно или несколько базовых преобразований алгоритма в произвольной среде программирования. Для проверки правильности реализации используются контрольные примеры, приведенные в ГОСТ Р 34.13-2015.

3. КОНТРОЛЬНЫЕ ЗАДАНИЯ

1. Перечислите основные режимы работы блочных шифров ГОСТ Р 34.12-2015.
2. Назовите процедуры дополнения открытого текста.
3. Какие из режимов шифрования не требуют дополнения исходного сообщения?
4. Какие режимы используют только функцию зашифрования?
5. Какие режимы предусматривают применения регистра сдвига?
6. Какие режимы предусматривают сжимающего преобразования?
7. Какие типы данных использовались в программной реализации?
8. Охарактеризуйте особенности программной реализации сжимающего преобразования.
9. Охарактеризуйте особенности программной реализации регистра сдвига.

Лабораторная работа 5.

Программная реализация компонентов функции хеширования «Стрибог» ГОСТ Р 34.11-2012

1. ЦЕЛЬ РАБОТЫ

Целью работы является изучение следующих элементов криптографических протоколов и стандартов:

- термины и определения.
- математический аппарат.
- базовые криптографические преобразования.
- программная реализация.

2. ПОРЯДОК ВЫПОЛНЕНИЯ РАБОТЫ

Лабораторная работа проводится в виде семинара с последующим выполнением программной реализации компонентов криптографического стандарта. Тематика семинара

соответствует теме лабораторной работы. Для подготовки следует использовать соответствующую литературу и источники сети Интернет. После обсуждения каждому студенту в соответствии с индивидуальным заданием предлагается реализовать одно или несколько базовых преобразований алгоритма в произвольной среде программирования. Для проверки правильности реализации используются контрольные примеры, приведенные в ГОСТ Р 34.11-2012.

3. КОНТРОЛЬНЫЕ ЗАДАНИЯ

1. Перечислите основные характеристики функции хэширования «Стрибог» ГОСТ Р 34.11-2012.
2. Сравните *S*-подстановки функции «Стрибог» и алгоритма шифрования «Кузнечик».
3. Охарактеризуйте раундовую функцию сжатия алгоритма.
4. Чем отличаются преобразования *LPSX* функции «Стрибог» и *LSX* алгоритма шифрования «Кузнечик»?
5. Какую процедуру дополнения исходного сообщения использует функция «Стрибог»?
6. В чем отличие функций хэширования с длинами сверток 256 и 512 бит?
7. Какие типы данных использовались в программной реализации?
8. Охарактеризуйте особенности программной реализации перестановки байт.
9. Охарактеризуйте особенности программной реализации линейного преобразования?

Лабораторная работа 6.

Построение криптографических протоколов с использованием ruToken CSP

1. ЦЕЛЬ РАБОТЫ

Целью работы является изучение следующих элементов прграммно-аппаратной реализации криптографических протоколов:

- архитектура ruToken CSP.
- мультиплатформенная библиотека высокого уровня PKCS#11ECP.

программное встраивание функций PKCS#11ECP, реализующих, базовые компоненты протоколов

2. ПОРЯДОК ВЫПОЛНЕНИЯ РАБОТЫ

Лабораторная работа проводится в виде семинара с последующим выполнением программной реализации компонентов криптографического протокола. Тематика семинара соответствует теме лабораторной работы. Для подготовки следует использовать соответствующую литературу и источники сети Интернет. После обсуждения каждому студенту в соответствии с индивидуальным заданием предлагается реализовать одно или несколько базовых преобразований алгоритма в среде программирования MS Visual Studio (Конфигурация C++) с использованием библиотеки PKCS#11ECP Rutoken SDK.

3. КОНТРОЛЬНЫЕ ЗАДАНИЯ

1. Перечислите основные этапы настройки и подключения PKCS#11ECP Rutoken SDK.
2. Назовите уровень интерфейса PKCS#11ECP.
3. Функции загрузки и инициализации PKCS#11ECP.
4. Опишите порядок подключения RutokenECP.
5. Функции управления объектами на токене.
6. Функции генерации ключей.
7. Вычисление значения хэш-функции
8. Функции симметричного шифрования.
9. Формирование электронной подписи.

Приложение 2

КОМПЛЕКТ ОЦЕНОЧНЫХ СРЕДСТВ К ЭКЗАМЕНУ

Грозненский государственный нефтяной технический университет
Институт цифровой экономики и технологического предпринимательства

Кафедра «Информационные системы в экономике»
Дисциплина «Информационная безопасность в цифровой экономике»
Билет №1

1. Разрушение оборудования или данных в результате небрежности.
2. Смена пользователей ПК, не соответствующая внутренним правилам

Преподаватель **М.К. Абдулаев**
Зав.кафедрой **Л.Р.Магомаева**

Грозненский государственный нефтяной технический университет
Институт цифровой экономики и технологического предпринимательства

Кафедра «Информационные системы в экономике»
Дисциплина «Информационная безопасность в цифровой экономике»
Билет №2

1. Риск нарушения ИБ
2. Разрушение оборудования или данных в результате небрежности.

Преподаватель **М.К. Абдулаев**
Зав.кафедрой **Л.Р.Магомаева**

Грозненский государственный нефтяной технический университет
Институт цифровой экономики и технологического предпринимательства

Кафедра «Информационные системы в экономике»
Дисциплина «Информационная безопасность в цифровой экономике»
Билет №3

1. Недостатки в документировании коммуникаций.
2. Уязвимости ПО или ошибки.

Преподаватель **М.К. Абдулаев**
Зав.кафедрой **Л.Р.Магомаева**

Грозненский государственный нефтяной технический университет
Институт цифровой экономики и технологического предпринимательства

Кафедра «Информационные системы в экономике»
Дисциплина «Информационная безопасность в цифровой экономике»
Билет №4

1. Запрещенные действия в информационной системе.
2. Опасности, связанные с увольнением или выведением персонала за штат.

Преподаватель **М.К. Абдулаев**
Зав.кафедрой **Л.Р.Магомаева**

Грозненский государственный нефтяной технический университет
Институт цифровой экономики и технологического предпринимательства

Кафедра «Информационные системы в экономике»
Дисциплина «Информационная безопасность в цифровой экономике»
Билет №5

1. Полный (Full) анализ рисков
2. Запрещенные действия системного администратора.

Преподаватель **М.К. Абдулаев**
Зав.кафедрой **Л.Р.Магомаева**

Грозненский государственный нефтяной технический университет
Институт цифровой экономики и технологического предпринимательства

Кафедра «Информационные системы в экономике»
Дисциплина «Информационная безопасность в цифровой экономике»
Билет №6

1. Неправильное администрирование сайта и прав доступа.
2. Полный (Full) анализ рисков

Преподаватель **М.К. Абдулаев**
Зав.кафедрой **Л.Р.Магомаева**

Грозненский государственный нефтяной технический университет
Институт цифровой экономики и технологического предпринимательства

Кафедра «Информационные системы в экономике»
Дисциплина «Информационная безопасность в цифровой экономике»
Билет №7

1. Полный (Full) анализ рисков
2. Неправильное администрирование сайта и прав доступа.

Преподаватель **М.К. Абдулаев**
Зав.кафедрой **Л.Р.Магомаева**

Грозненский государственный нефтяной технический университет
Институт цифровой экономики и технологического предпринимательства

Кафедра «Информационные системы в экономике»
Дисциплина «Информационная безопасность в цифровой экономике»
Билет №8

1. Неправильное хранение носителей информации в случае аварий.
2. Неправильное администрирование сайта и прав доступа.

Преподаватель **М.К. Абдулаев**
Зав.кафедрой **Л.Р.Магомаева**

Грозненский государственный нефтяной технический университет
Институт цифровой экономики и технологического предпринимательства

Кафедра «Информационные системы в экономике»
Дисциплина «Информационная безопасность в цифровой экономике»
Билет №9

1. Нарушение правил администрирования DBMS
2. Недостатки системы сегментации.

Преподаватель **М.К. Абдулаев**
Зав.кафедрой **Л.Р.Магомаева**

Грозненский государственный нефтяной технический университет
Институт цифровой экономики и технологического предпринимательства

Кафедра «Информационные системы в экономике»
Дисциплина «Информационная безопасность в цифровой экономике»
Билет №10

1. Источник угрозы
2. Запрещенные действия системного администратора.

Преподаватель **М.К. Абдулаев**
Зав.кафедрой **Л.Р.Магомаева**