

Министерство науки и высшего образования Российской Федерации
Нижекамский химико-технологический институт (филиал)
федерального государственного бюджетного образовательного учреждения
высшего образования
«Казанский национальный исследовательский технологический университет»
(НХТИ ФГБОУ ВО «КНИТУ»)



УТВЕРЖДАЮ

Заместитель директора по УР

Н.И. Никифорова

« 12 » апреля 2021 г.

ФОНД ОЦЕНОЧНЫХ СРЕДСТВ

по дисциплине (модулю)

Б1.О.23 Защита информации

(код и наименование дисциплины (модуля))

09.03.01 «Информатика и вычислительная техника»

(код и наименование направления подготовки/специальности)

Автоматизированные системы обработки информации и управления

(наименование профиля/специализации)

бакалавр

квалификация

форма обучения очная, очно-заочная, заочная

Нижнекамск 2021

Составитель ФОС:
Ст. преподаватель


(подпись)

Захарова И.Н.

ФОС рассмотрен и одобрен на заседании кафедры ИСТ,
протокол от 15.03.2021 г. № 7.

Зав. кафедрой


(подпись)

Матухина О.В.

Эксперт:

Руководитель ООП
ст. преподаватель кафедры ИСТ


(подпись)

Амаева Л.А.

Перечень компетенций и индикаторов достижения компетенций с указанием этапов формирования в процессе освоения дисциплины

ОПК-2 Способен использовать современные информационные технологии и программные средства, в том числе отечественного производства, при решении задач профессиональной деятельности;

ОПК-2.1 Знает современные информационные технологии и программные средства, в том числе отечественного производства, при решении задач профессиональной деятельности

ОПК-2.2 Умеет выбирать современные информационные технологии и программные средства, в том числе отечественного производства, при решении задач профессиональной деятельности

ОПК-2.3 Владеет навыками применения современных информационных технологий и программных средств, в том числе отечественного производства, при решении задач профессиональной деятельности

ОПК-3 Способен решать стандартные задачи профессиональной деятельности на основе информационной и библиографической культуры с применением информационно-коммуникационных технологий и с учетом основных требований информационной безопасности;

ОПК-3.1 Знает принципы, методы и средства решения стандартных задач профессиональной деятельности на основе информационной и библиографической культуры с применением информационно-коммуникационных технологий и с учетом основных требований информационной безопасности

ОПК-3.2 Умеет решать стандартные задачи профессиональной деятельности на основе информационной и библиографической культуры с применением информационнокоммуникационных технологий и с учетом основных требований информационной безопасности

ОПК-3.3 Владеет навыками подготовки обзоров, аннотаций, составления рефератов, научных докладов, публикаций, и библиографии по научноисследовательской работе с учетом требований информационной безопасности

ОПК-6 Способен разрабатывать бизнес-планы и технические задания на оснащение отделов, лабораторий, офисов компьютерным и сетевым оборудованием;

ОПК-6.1 Знает принципы формирования и структуру бизнес-планов и технических заданий на оснащение отделов, лабораторий, офисов компьютерным и сетевым оборудованием

ОПК-6.2 Умеет разрабатывать бизнес-планы и технические задания на оснащение отделов, лабораторий, офисов компьютерным и сетевым оборудованием

ОПК-6.3 Владеет навыками разработки бизнес-планов и технических заданий на оснащение отделов, лабораторий, офисов компьютерным и сетевым оборудованием

ОПК-9 Способен осваивать методики использования программных средств для решения практических задач.

ОПК-9.1 Знает методики использования программных средств для решения практических задач

ОПК-9.2 Умеет использовать программные средства для решения практических задач

ОПК-9.3 Владеет навыками использования программных средств для решения практических задач

Индекс Компетен- ции	Этапы формирования компетенции (указать все темы из РПД)				Наименование оценочного сред- ства
	Лекции	Практические Занятия, лаборатор- ный практикум	Лаборатор- ные занятия	Курсовой проект (работа)	
ОПК-2.1	Тема 1-- 12	Не предусмотрены	Лаб.зан. 1-10	Не предусмотрены	Экзамен, реферат, расчетно-графиче- ская работа/контрольная работа
ОПК-2.2	-	Не предусмотрены	Лаб.зан. 1-10	Не предусмотрены	Экзамен, реферат, расчетно-графиче- ская работа/контрольная работа
ОПК-2.3	-	Не предусмотрены	Лаб.зан. 1-10	Не предусмотрены	Экзамен, реферат, расчетно-графиче- ская работа/контрольная работа
ОПК-3.1	Тема 1-- 12	Не предусмотрены	Лаб.зан. 1-10	Не предусмотрены	Экзамен, реферат, расчетно-графиче- ская работа/контрольная работа
ОПК-3.2	-	Не предусмотрены	Лаб.зан. 1-10	Не предусмотрены	Экзамен, реферат, расчетно-графиче- ская работа/контрольная работа
ОПК-3.3	-	Не предусмотрены	Лаб.зан. 1-10	Не предусмотрены	Экзамен, реферат, расчетно-графиче- ская работа/контрольная работа
ОПК-6.1	Тема 1-- 12	Не предусмотрены	Лаб.зан. 1-10	Не предусмотрены	Экзамен, реферат, расчетно-графиче- ская работа/контрольная работа
ОПК-6.2	-	Не предусмотрены	Лаб.зан. 1-10	Не предусмотрены	Экзамен, реферат, расчетно-графиче- ская работа/контрольная работа
ОПК-6.3	-	Не предусмотрены	Лаб.зан. 1-10	Не предусмотрены	Экзамен, реферат, расчетно-графиче- ская работа/контрольная работа
ОПК-9.1	Тема 1-- 12	Не предусмотрены	Лаб.зан. 1-10	Не предусмотрены	Экзамен, реферат, расчетно-графиче- ская работа/контрольная работа
ОПК-9.2	-	Не предусмотрены	Лаб.зан. 1-10	Не предусмотрены	Экзамен, реферат, расчетно-графиче- ская работа/контрольная работа
ОПК-9.3	-	Не предусмотрены	Лаб.зан. 1-10	Не предусмотрены	Экзамен, реферат, расчетно-графиче- ская работа

Перечень оценочных средств по дисциплине (модулю)

При оценке результатов деятельности обучающихся в рамках дисциплины «Защита информации» используется рейтинговая система. Рейтинговая оценка формируется на основании текущего и промежуточного контроля. Максимальное и минимальное количество баллов по различным видам учебной работы описано в «Положении о балльно-рейтинговой системе оценки знаний студентов и обеспечения качества учебного процесса» ФГБОУ ВО «КНИТУ».

При изучении дисциплины предусматривается экзамен, реферат, выполнение двух расчётно-графических работ. За эти контрольные точки студент может получить минимальное и максимальное количество баллов (см. таблицу).

За экзамен студент может получить минимум 24 балла и максимум – 40 баллов.

Очная, очно-заочная форма

Оценочные средства	Кол-во	Min, баллов	Max, баллов
Расчётно-графических работа	2	20	40
Групповой проект	1	8	10
Реферат	1	8	10
Экзамен	1	24	40
Итого:		60	100

Заочная форма

<i>Оценочные средства</i>	<i>Кол-во</i>	<i>Min, баллов (базовый уровень)</i>	<i>Max, баллов (повышенный уровень)</i>
<i>Контрольная работа</i>	<i>1</i>	<i>36</i>	<i>60</i>
<i>Экзамен</i>	<i>1</i>	<i>24</i>	<i>40</i>
<i>Итого:</i>		<i>60</i>	<i>100</i>

Шкала оценивания

Цифровое выражение	Выражение в баллах:	Словесное выражение	Критерии оценки индикаторов достижения при форме контроля:
			экзамен
5	87 - 100	Отлично (зачтено)	Оценка «отлично» выставляется студенту, если теоретическое содержание курса освоено полностью, без пробелов; исчерпывающе, последовательно, четко и логически стройно излагает материал; свободно справляется с задачами, вопросами и другими видами применения знаний; использует в ответе дополнительный материал все предусмотренные программой задания выполнены, качество их выполнения оценено числом баллов, близким к максимальному; анализирует полученные результаты; проявляет самостоятельность при выполнении заданий

4	74 - 86	Хорошо (зачтено)	Оценка «хорошо» выставляется студенту, если теоретическое содержание курса освоено полностью, необходимые практические компетенции в основном сформированы, все предусмотренные программой обучения учебные задания выполнены, качество их выполнения достаточно высокое. Студент твердо знает материал, грамотно и по существу излагает его, не допуская существенных неточностей в ответе на вопрос.
3	60 - 73	Удовлетворительно (зачтено)	Оценка «удовлетворительно» выставляется студенту, если теоретическое содержание курса освоено частично, но пробелы не носят существенного характера, большинство предусмотренных программой заданий выполнено, но в них имеются ошибки, при ответе на поставленный вопрос студент допускает неточности, недостаточно правильные формулировки, наблюдаются нарушения логической последовательности в изложении программного материала.
2	Ниже 60	Неудовлетворительно (не зачтено)	Оценка «неудовлетворительно» выставляется студенту, если он не знает значительной части программного материала, допускает существенные ошибки, неуверенно, с большими затруднениями выполняет практические работы, необходимые практические компетенции не сформированы, большинство предусмотренных программой обучения учебных заданий не выполнено, качество их выполнения оценено числом баллов, близким к минимальному

Министерство науки и высшего образования Российской Федерации
Нижекамский химико-технологический институт (филиал)
федерального государственного бюджетного образовательного учреждения
высшего образования
«Казанский национальный исследовательский технологический университет»

Факультет Управления и автоматизации

Кафедра Информационных систем и технологий

Направление подготовки/специальность: 09.03.01 «Информатика и вычислительная техника»

Профиль/специализация: Автоматизированные системы обработки информации и управления

Комплект заданий для выполнения расчетно-графической работы
по дисциплине Б1.В.11 «Защита информации»
(наименование дисциплины)

Задание 1. Выполните первый цикл алгоритма шифрования ГОСТ 28147-89 в режиме простой замены. Для получения 64 бит исходного текста используйте 8 первых букв из своих данных: Фамилии Имени Отчества. Для получения ключа (256 бит) используют текст, состоящий из 32 букв. Первый подключ содержит первые 4 буквы.

Требования к выполнению. Описать:

- алгоритм шифрования.
- схема шифрования и дешифрования;
- достоинства, недостатки;
- где используется;

Решить задачу аналитическим способом. Написать программу на Языке высокого уровня. Сравнить результаты полученные программой и аналитическим способом. Сделать выводы.

Задание 2. Сгенерируйте открытый и закрытый ключи в алгоритме шифрования RSA, выбрав простые числа p (последняя цифра даты вашего рождения) и q (месяц вашего рождения). Зашифруйте сообщение, состоящее из вашего имени (по паспорту).

Требования к выполнению. Описать:

- алгоритм шифрования.
- схема шифрования и дешифрования;

- достоинства, недостатки;
- где используется;

Решить задачу аналитическим способом. Реализовать алгоритм шифрования RSA в табличном процессоре. Сравнить результаты полученные программой и аналитическим способом. Сделать выводы.

№	Количество баллов	Критерии оценивания
1	20 баллов	работа выполнена полностью; в логических рассуждениях и обосновании решения нет пробелов и ошибок; в построении алгоритма решения нет ошибок (возможны некоторые неточности, опiski, которая не является следствием незнания или непонимания учебного материала), т.е. правильно выполнено 86–100% работы.
2	16 баллов	работа выполнена полностью, но обоснования шагов решения недостаточны; допущены одна ошибка, или есть два – три недочёта при шифровании, дешифровании текста , т.е. правильно выполнено 74 – 85 % работы.
3	12 баллов	допущено не более двух ошибок при шифровании, дешифровании текста , но обучающийся обладает обязательными умениями по проверяемой теме, т.е. правильно выполнено 60 – 73 % работы.

Министерство науки и высшего образования Российской Федерации
Нижекамский химико-технологический институт (филиал)
федерального государственного бюджетного образовательного учреждения
высшего образования
«Казанский национальный исследовательский технологический университет»

Факультет Управления и автоматизации

Кафедра Информационных систем и технологий

Направление подготовки/специальность: 09.03.01 «Информатика и вычислительная техника»

Профиль/специализация: Автоматизированные системы обработки информации и управления

Темы рефератов по дисциплине Информационная безопасность систем управления технологическими процессами

(наименование дисциплины)

Раздел 2. Модели политик безопасности

Варианты тем:

1. Модель Кларка Вилсона
2. Модель «Китайская стена»
3. Модель Белла и Ла Падуллы
4. Модель Гогена-Мезигера
5. Сазерлендская модель
6. Дискреционная (матричная) модель
7. Модель Take-Grant
8. Модель типизированной матрицы доступа (Модель Харрисона-Руззо-Ульмана)
9. Модель Диона
10. Модель Биба
11. Ролевая политика

Критерии оценки реферата:

Структура реферата:

- 1) титульный лист;
- 2) план работы с указанием страниц каждого вопроса, подвопроса (пункта);
- 3) введение;
- 4) текстовое изложение материала, разбитое на вопросы и подвопросы (пункты,

- подпункты) с необходимыми ссылками на источники, использованные автором;
- 5) заключение;
 - 6) список использованной литературы;
 - 7) приложения, которые состоят из таблиц, диаграмм, графиков, рисунков, схем (необязательная часть реферата).

Приложения располагаются последовательно, согласно заголовкам, отражающим их содержание.

Реферат оценивается научным руководителем исходя из установленных кафедрой показателей и критериев оценки реферата.

Критерии и показатели, используемые при оценивании учебного реферата

Критерии	Показатели
1. Новизна реферированного текста Макс. - 3 балла	<ul style="list-style-type: none"> - актуальность проблемы и темы; - новизна и самостоятельность в постановке проблемы, в формулировании нового аспекта выбранной для анализа проблемы; - наличие авторской позиции, самостоятельность суждений.
2. Степень раскрытия сущности проблемы Макс. - 2 балла	<ul style="list-style-type: none"> - соответствие плана теме реферата; - соответствие содержания теме и плану реферата; - полнота и глубина раскрытия основных понятий проблемы; - обоснованность способов и методов работы с материалом; - умение работать с литературой, систематизировать и структурировать материал; - умение обобщать, сопоставлять различные точки зрения по рассматриваемому вопросу, аргументировать основные положения и выводы.
3. Обоснованность выбора источников Макс. - 2 балла	<ul style="list-style-type: none"> - круг, полнота использования литературных источников по проблеме; - привлечение новейших работ по проблеме (журнальные публикации, материалы сборников научных трудов и т.д.).
4. Соблюдение требований к оформлению Макс. - 1 балла	<ul style="list-style-type: none"> - правильное оформление ссылок на используемую литературу; - грамотность и культура изложения; - владение терминологией и понятийным аппаратом

	проблемы; - соблюдение требований к объему реферата; - культура оформления: выделение абзацев.
5. Грамотность Макс. - 1 балла	- отсутствие орфографических и синтаксических ошибок, стилистических погрешностей; - отсутствие опечаток, сокращений слов, кроме общепринятых; - литературный стиль.
6. Проверка на антиплагиат Макс.1 баллов	- проверка реферата в система антиплагиат. - должно быть не менее 70% оригинальности текста

Министерство науки и высшего образования Российской Федерации
Нижекамский химико-технологический институт (филиал)
федерального государственного бюджетного образовательного учреждения
высшего образования
«Казанский национальный исследовательский технологический университет»

Факультет Управления и автоматизации

Кафедра Информационных систем и технологий

Направление подготовки/специальность: 09.03.01 «Информатика и вычислительная техника»

Профиль/специализация: Автоматизированные системы обработки информации и управления

Групповое творческое задание №1

Тема: Информационная безопасность промышленной сети.

Требования:

Создать проект промышленной сети своего предприятия. Описать применяемый программно-аппаратный комплекс. Обосновать выбор проектного решения. Работа группы обучающихся над проектом должна быть осуществлена с применением облачных технологий. Необходимо создать публичное облако в сети интернет. Преподаватель-эксперт наблюдает за работой группы, и при необходимости координирует работу группы удаленно (через публичное облако). Группа совместно с преподавателем ведет рейтинг активности каждого обучающегося.

Разделы проекта:


1. Постановка задачи (назначение, основные задачи сети)
2. Конструкторская часть
 - 2.1.Технология построения
 - 2.2.Топология сети
 - 2.3.Метод доступа
 - 2.4.Аппаратное обеспечение. Информационная безопасность сети.
 - 2.5.Программное обеспечение управления сетью. Информационная безопасность рабочих станций, сервера.
 - 2.6. Интернет-технологии АСУТП. Защита информации в сети интернет.

Критерии оценки:

№	Количество баллов	Критерии оценивания
1	10 баллов	При выполнении творческого задания, обучающийся активно использовал интернет-технологии, в процессе выполнения работы, преподаватель был наблюдателем; работа выполнена полностью; в логических рассуждениях и обосновании решения нет пробелов и ошибок; в построении моделей нет ошибок (возможны некоторые неточности, описки, которая не является следствием незнания или непонимания учебного материала); т.е. правильно выполнено 86–100% работы.
2	9 баллов	При выполнении творческого задания, обучающийся активно использовал интернет-технологии, в процессе выполнения работы, преподаватель координировал проектные решения; работа выполнена полностью, но обоснования шагов решения недостаточны; допущена одна ошибка, или есть два – три недочёта при проектировании, недочёты в программном коде приложения при реализации запросов, т.е. правильно выполнено 74 – 85 % работы.
3	8 баллов	При выполнении творческого задания обучающийся активно использовал интернет-технологии, в процессе выполнения работы, преподаватель активно координировал проектные решения; допущено не более двух ошибок при проектировании или более двух – трех недочетов в изображениях моделей, при исполнении приложения ЭС, но обучающийся обладает обязательными умениями по проверяемой теме, т.е. правильно выполнено 60 – 73 % работы.

Министерство науки и высшего образования Российской Федерации
Нижекамский химико-технологический институт (филиал) федерального государственного бюджетного образовательного учреждения
высшего образования
«Казанский национальный исследовательский технологический университет»
Факультет ИТ
Кафедра Информационных систем и технологий
Направление подготовки/специальность: 09.03.01 «Информатика и вычислительная техника»
Профиль: Автоматизированные системы обработки информации и управления

УТВЕРЖДАЮ
Зав. кафедрой ИСТ

 (подпись) О.В. Матухина

« 15 » 03 2021 г.

Экзаменационный билет № 1

1. Угрозы безопасности информации и их классификация
2. Понятие идентификации и аутентификации


Составитель

 (подпись)

И.Н. Захарова

Министерство науки и высшего образования Российской Федерации
Нижекамский химико-технологический институт (филиал) федерального государственного бюджетного образовательного учреждения
высшего образования
«Казанский национальный исследовательский технологический университет»
Факультет ИТ
Кафедра Информационных систем и технологий
Направление подготовки/специальность: 09.03.01 «Информатика и вычислительная техника»
Профиль: Автоматизированные системы обработки информации и управления

УТВЕРЖДАЮ
Зав. кафедрой ИСТ

 (подпись) О.В. Матухина

« 15 » 03 2021 г.

Экзаменационный билет № 2

1. Принципы проектирования систем защиты информации
2. Модели политик безопасности. Политика безопасности Белла-ЛаПадулла

Составитель

 (подпись)

И.Н. Захарова

Министерство науки и высшего образования Российской Федерации
Нижекамский химико-технологический институт (филиал) федерального государственного бюджетного образовательного учреждения
высшего образования
«Казанский национальный исследовательский технологический университет»
Факультет ИТ
Кафедра Информационных систем и технологий
Направление подготовки/специальность: 09.03.01 «Информатика и вычислительная техника»

Профиль: Автоматизированные системы обработки информации и управления

УТВЕРЖДАЮ

Зав. кафедрой ИСТ


(подпись)

О.В. Матухина

« 15 » 03 2021 г.

Экзаменационный билет № 3

1. Парольная подсистема идентификации и аутентификации в ОС Windows.
2. Электронная цифровая подпись

Составитель


(подпись)

И.Н. Захарова

Министерство науки и высшего образования Российской Федерации
Нижекамский химико-технологический институт (филиал) федерального государственного бюджетного образовательного учреждения
высшего образования
«Казанский национальный исследовательский технологический университет»
Факультет ИТ
Кафедра Информационных систем и технологий
Направление подготовки/специальность: 09.03.01 «Информатика и вычислительная техника»

Профиль: Автоматизированные системы обработки информации и управления

УТВЕРЖДАЮ

Зав. кафедрой ИСТ


(подпись)

О.В. Матухина

« 15 » 03 2021 г.

Экзаменационный билет № 4

1. Политики безопасности от нарушения целостности информации. Политика безопасности Биба.
2. Физические устройства идентификации и аутентификации


Составитель


(подпись)

И.Н. Захарова

Министерство науки и высшего образования Российской Федерации
Нижекамский химико-технологический институт (филиал) федерального государственного бюджетного образовательного учреждения
высшего образования
«Казанский национальный исследовательский технологический университет»
Факультет ИТ
Кафедра Информационных систем и технологий
Направление подготовки/специальность: 09.03.01 «Информатика и вычислительная техника»
Профиль: Автоматизированные системы обработки информации и управления

УТВЕРЖДАЮ
Зав. кафедрой ИСТ

 О.В. Матухина
(подпись)

« 15 » 03 2021 г.

Экзаменационный билет № 5

1. Биометрические подсистемы идентификации и аутентификации.
2. Простейшие криптографические алгоритмы


Составитель

 (подпись)

И.Н. Захарова

Министерство науки и высшего образования Российской Федерации
Нижекамский химико-технологический институт (филиал) федерального государственного бюджетного образовательного учреждения
высшего образования
«Казанский национальный исследовательский технологический университет»
Факультет ИТ
Кафедра Информационных систем и технологий
Направление подготовки/специальность: 09.03.01 «Информатика и вычислительная техника»
Профиль: Автоматизированные системы обработки информации и управления

УТВЕРЖДАЮ
Зав. кафедрой ИСТ

 О.В. Матухина
(подпись)

« 15 » 03 2021 г.

Экзаменационный билет № 6

1. Защита программного обеспечения от несанкционированного использования
2. Функции хэширования.


Составитель

 (подпись)

И.Н. Захарова

Министерство науки и высшего образования Российской Федерации
Нижекамский химико-технологический институт (филиал) федерального государственного бюджетного образовательного учреждения
высшего образования
«Казанский национальный исследовательский технологический университет»
Факультет ИТ
Кафедра Информационных систем и технологий
Направление подготовки/специальность: 09.03.01 «Информатика и вычислительная техника»
Профиль: Автоматизированные системы обработки информации и управления

УТВЕРЖДАЮ
Зав. кафедрой ИСТ


(подпись) О.В. Матухина

« 15 » 03 2021 г.

Экзаменационный билет № 7

1. Стандартизация и сертификация в области защиты информации.
2. Симметричные криптосистемы.


Составитель


(подпись)

И.Н. Захарова

Министерство науки и высшего образования Российской Федерации
Нижекамский химико-технологический институт (филиал) федерального государственного бюджетного образовательного учреждения
высшего образования
«Казанский национальный исследовательский технологический университет»
Факультет ИТ
Кафедра Информационных систем и технологий
Направление подготовки/специальность: 09.03.01 «Информатика и вычислительная техника»
Профиль: Автоматизированные системы обработки информации и управления

УТВЕРЖДАЮ
Зав. кафедрой ИСТ


(подпись) О.В. Матухина

« 15 » 03 2021 г.

Экзаменационный билет № 8

1. Асимметричные криптосистемы
2. Защита баз данных аутентификации ОС. Аудит


Составитель


(подпись)

И.Н. Захарова

Министерство науки и высшего образования Российской Федерации
Нижекамский химико-технологический институт (филиал) федерального государственного бюджетного образовательного учреждения
высшего образования
«Казанский национальный исследовательский технологический университет»
Факультет ИТ
Кафедра Информационных систем и технологий
Направление подготовки/специальность: 09.03.01 «Информатика и вычислительная техника»
Профиль: Автоматизированные системы обработки информации и управления

УТВЕРЖДАЮ
Зав. кафедрой ИСТ

 О.В. Матухина
(подпись)

« 15 » 03 2021 г.

Экзаменационный билет № 9

1. Разрушающие программные воздействия, защита от них
2. Электронно-цифровая подпись


Составитель

 (подпись)

И.Н. Захарова

Министерство науки и высшего образования Российской Федерации
Нижекамский химико-технологический институт (филиал) федерального государственного бюджетного образовательного учреждения
высшего образования
«Казанский национальный исследовательский технологический университет»
Факультет ИТ
Кафедра Информационных систем и технологий
Направление подготовки/специальность: 09.03.01 «Информатика и вычислительная техника»
Профиль: Автоматизированные системы обработки информации и управления

УТВЕРЖДАЮ
Зав. кафедрой ИСТ

 О.В. Матухина
(подпись)

« 15 » 03 2021 г.

Экзаменационный билет № 10

1. Алгоритм шифрования ГОСТ 34.12-2015
2. Системы обнаружения вторжений.


Составитель

 (подпись)

И.Н. Захарова

Министерство науки и высшего образования Российской Федерации
Нижекамский химико-технологический институт (филиал) федерального государственного бюджетного образовательного учреждения
высшего образования
«Казанский национальный исследовательский технологический университет»
Факультет ИТ
Кафедра Информационных систем и технологий
Направление подготовки/специальность: 09.03.01 «Информатика и вычислительная техника»
Профиль: Автоматизированные системы обработки информации и управления

УТВЕРЖДАЮ
Зав. кафедрой ИСТ

 (подпись) О.В. Матухина

« 15 » 03 2021 г.

Экзаменационный билет № 11

1. *Российский стандарт ЭП ГОСТ 32.10-94*
2. *Модульная схема подсистемы защиты ПО от несанкционированной информации.*


Составитель

 (подпись)

И.Н. Захарова

Министерство науки и высшего образования Российской Федерации
Нижекамский химико-технологический институт (филиал) федерального государственного бюджетного образовательного учреждения
высшего образования
«Казанский национальный исследовательский технологический университет»
Факультет ИТ
Кафедра Информационных систем и технологий
Направление подготовки/специальность: 09.03.01 «Информатика и вычислительная техника»
Профиль: Автоматизированные системы обработки информации и управления

УТВЕРЖДАЮ
Зав. кафедрой ИСТ

 (подпись) О.В. Матухина

« 15 » 03 2021 г.

Экзаменационный билет № 12

1. *Виды угроз и каналы утечки информации в корпоративных сетях*
2. *Методы защиты информации*

Составитель

 (подпись)

И.Н. Захарова

Министерство науки и высшего образования Российской Федерации
Нижекамский химико-технологический институт (филиал)
федерального государственного бюджетного образовательного учреждения
высшего образования
«Казанский национальный исследовательский технологический университет»

Факультет Управления и автоматизации

Кафедра Информационных систем и технологий

Направление подготовки/специальность: 09.03.01 «Информатика и вычислительная техника»

Профиль/специализация: Автоматизированные системы обработки информации и управления

**Комплект заданий для выполнения контрольной работы
(заочная форма)**

по дисциплине Б1.В.11 «Защита информации»

(наименование дисциплины)

Задание 1. Выполните первый цикл алгоритма шифрования ГОСТ 28147-89 в режиме простой замены. Для получения 64 бит исходного текста используйте 8 первых букв из своих данных: Фамилии Имени Отчества. Для получения ключа (256 бит) используют текст, состоящий из 32 букв. Первый подключ содержит первые 4 буквы.

Требования к выполнению. Описать:

- алгоритм шифрования.
- схема шифрования и дешифрования;
- достоинства, недостатки;
- где используется;

Решить задачу аналитическим способом. Написать программу на Языке высокого уровня. Сравнить результаты полученные программой и аналитическим способом. Сделать выводы.

Задание 2. Сгенерируйте открытый и закрытый ключи в алгоритме шифрования RSA, выбрав простые числа p (последняя цифра даты вашего рождения) и q (месяц вашего рождения). Зашифруйте сообщение, состоящее из вашего имени (по паспорту).

Требования к выполнению. Описать:

- алгоритм шифрования.
- схема шифрования и дешифрования;

- достоинства, недостатки;
- где используется;

Решить задачу аналитическим способом. Реализовать алгоритм шифрования RSA в табличном процессоре. Сравнить результаты, полученные программой и аналитическим способом. Сделать выводы.

Критерии оценки

№	Количество баллов	Критерии оценивания
1	60 баллов	работа выполнена полностью; в логических рассуждениях и обосновании решения нет пробелов и ошибок; в построении алгоритма решения нет ошибок (возможны некоторые неточности, описки, которая не является следствием незнания или непонимания учебного материала), т.е. правильно выполнено 86–100% работы.
2	55 баллов	работа выполнена полностью, но обоснования шагов решения недостаточны; допущены одна ошибка, или есть два – три недочёта при шифровании, дешифровании текста, т.е. правильно выполнено 74 – 85 % работы.
3	36 баллов	допущено не более двух ошибок при шифровании, дешифровании текста, но обучающийся обладает обязательными умениями по проверяемой теме, т.е. правильно выполнено 60 – 73 % работы.