СТЕРЛИТАМАКСКИЙ ФИЛИАЛ
ФЕДЕРАЛЬНОГО ГОСУДАРСТВЕННОГО БЮДЖЕТНОГО ОБРАЗОВАТЕЛЬНОГО
УЧРЕЖДЕНИЯ ВЫСШЕГО ОБРАЗОВАНИЯ
«УФИМСКИЙ УНИВЕРСИТЕТ НАУКИ И ТЕХНОЛОГИЙ»

Факультет ***Математики и информационных технологий***
Кафедра ***Математического моделирования***

Оценочные материалы по дисциплине (модулю)

дисциплина ***Основы информационной безопасности***

Блок Б1, обязательная часть, Б1.О.26
цикл дисциплины и его часть (обязательная часть или часть, формируемая участниками образовательных отношений)

Направление

01.03.02 ***Прикладная математика и информатика***
код наименование направления

Программа

Искусственный интеллект и анализ данных

Форма обучения

Очная

Для поступивших на обучение в
2023 г.

Разработчик (составитель)
к.ф.-м.н., доцент
Викторов С. В.
ученая степень, должность, ФИО

Стерлитамак 2023

1. Перечень компетенций, индикаторов достижения компетенций и описание показателей и критериев оценивания результатов обучения по дисциплине (модулю) 3

2. Оценочные средства, необходимые для оценки результатов обучения по дисциплине (модулю).....8

3. Методические материалы, определяющие процедуры оценивания результатов обучения по дисциплине (модулю), описание шкал оценивания 33

1. Перечень компетенций, индикаторов достижения компетенций и описание показателей и критериев оценивания результатов обучения по дисциплине (модулю)

Формируемая компетенция (с указанием кода)	Код и наименование индикатора достижения компетенции	Результаты обучения по дисциплине (модулю)	Показатели и критерии оценивания результатов обучения по дисциплине (модулю)				Вид оценочного средства
1	2	3	4				5
			неуд.	удовл.	хорошо	отлично	
УК-2. Способен определять круг задач в рамках поставленной цели и выбирать оптимальные способы их решения, исходя из действующих правовых норм, имеющихся ресурсов и ограничений	УК-2.1. Реализует нормы права при решении задач в рамках поставленной цели	Обучающийся должен: знать правовые нормы и методологические основы принятия управленческого решения	Не знает правовых норм и методологических основ принятия управленческого решения	Фрагментарное знание правовых норм и методологических основ принятия управленческого решения	В целом успешное, но содержащее отдельные пробелы знание правовых норм и методологических основ принятия управленческого решения	Успешное систематическое знание правовых норм и методологических основ принятия управленческого решения	Устный опрос
	УК-2.2. Умеет проводить анализ поставленной цели и формулировать задачи, которые необходимо решить для ее достижения;	Обучающийся должен: уметь анализировать альтернативные варианты решений для достижения намеченных результатов; разрабатывать	Не уметь анализировать альтернативные варианты решений для достижения намеченных результатов; разрабатывать план,	Фрагментарное умение анализировать альтернативные варианты решений для достижения намеченных результатов; разрабатывать	В целом успешное, но содержащее отдельные пробелы умение анализировать альтернативные варианты решений для достижения	Успешное систематическое умение анализировать альтернативные варианты решений для достижения намеченных результатов;	Тестовые задания

	анализировать альтернативные варианты для достижения намеченных результатов; использовать нормативно-правовую документацию в сфере профессиональной деятельности	план, определять целевые этапы и основные направления работ.	определять целевые этапы и основные направления работ.	план, определять целевые этапы и основные направления работ.	намеченных результатов; разрабатывать план, определять целевые этапы и основные направления работ.	разрабатывать план, определять целевые этапы и основные направления работ.	
	УК-2.3. Владеет методиками разработки цели и задач проекта; методами оценки потребности в ресурсах, продолжительности и стоимости проекта; навыками работы с нормативно правовой документацией	Обучающийся должен: владеть методиками разработки цели и задач проекта; методами оценки продолжительности и стоимости проекта, а также потребности в ресурсах.	Не владеет методиками разработки цели и задач проекта; методами оценки продолжительности и стоимости проекта, а также потребности в ресурсах.	Фрагментарное владение методиками разработки цели и задач проекта; методами оценки продолжительности и стоимости проекта, а также потребности в ресурсах.	В целом успешное, но содержащее отдельные пробелы владение методиками разработки цели и задач проекта; методами оценки продолжительности и стоимости проекта, а также потребности в ресурсах.	Успешное систематическое владение методиками разработки цели и задач проекта; методами оценки продолжительности и стоимости проекта, а также потребности в ресурсах.	Контрольная работа
ОПК-4. Способен	ОПК-4.1. знать и понимать	Обучающийся должен: знать	Не знает способы	Фрагментарное знание способов	В целом успешно, но	Успешное систематическо	Устный опрос

понимать принципы работы современных информационных технологий и использовать их для решения задач профессиональной деятельности	принципы работы современных информационных технологий и программных средств, в том числе отечественного производства при решении задач профессиональной деятельности	способы получения на основе информационных технологий новых знаний для решения профессиональных задач с учетом требований информационной безопасности и причин нарушения безопасности компьютерных систем.	получения на основе информационных технологий новых знаний для решения профессиональных задач с учетом требований информационной безопасности и причин нарушения безопасности компьютерных систем.	получения на основе информационных технологий новых знаний для решения профессиональных задач с учетом требований информационной безопасности и причин нарушения безопасности компьютерных систем	содержащее отдельные пробелы знание способов получения на основе информационных технологий новых знаний для решения профессиональных задач с учетом требований информационной безопасности и причин нарушения безопасности компьютерных систем	е знание способов получения на основе информационных технологий новых знаний для решения профессиональных задач с учетом требований информационной безопасности и причин нарушения безопасности компьютерных систем	
	ОПК-4.2. уметь выбирать современные информационные технологии и программные средства, в том числе отечественного производства при решении	Обучающийся должен: уметь применять информационные технологии и программные средства, в том числе отечественного производства,	Не умеет применять информационные технологии и программные средства, в том числе отечественного производства, для анализа и оценивания	Фрагментарное умение применять информационные технологии и программные средства, в том числе отечественного производства, для анализа и	В целом успешное, но содержащее отдельные пробелы умение применять информационные технологии и программные средства, в том числе	Успешное систематическое умение применять информационные технологии и программные средства, в том числе отечественного производства,	Тестовые задания

	задач профессиональной деятельности	для анализа и оценивания эффективности средств защиты информации; ориентироватьс я в современных и перспективных методах защиты информации.	эффективности средств защиты информации; ориентироватьс я в современных и перспективных методах защиты информации.	оценивания эффективности средств защиты информации; ориентироватьс я в современных и перспективных методах защиты информации.	отечественного производства, для анализа и оценивания эффективности средств защиты информации; ориентироватьс я в современных и перспективных методах защиты информации.	для анализа и оценивания эффективности средств защиты информации; ориентироватьс я в современных и перспективных методах защиты информации.	
	ОПК-4.3. иметь практический опыт применения современных информационны х технологий и программных средств, в том числе отечественного производства, при решении задач профессиональн ой деятельности	Обучающийся должен: владеть навыками применения методов защиты информации в компьютерных системах; иметь практический опыт применения современных информационны х технологий и программных средств, в том числе отечественного	Не владеет навыками применения методов защиты информации в компьютерных системах; иметь практический опыт применения современных информационны х технологий и программных средств, в том числе отечественного производства, при решении	Фрагментарное владение навыками применения методов защиты информации в компьютерных системах; иметь практический опыт применения современных информационны х технологий и программных средств, в том числе отечественного производства,	В целом успешное, но содержащее отдельные пробелы владение навыками применения методов защиты информации в компьютерных системах; иметь практический опыт применения современных информационны х технологий и программных	Успешное систематическо е владение навыками применения методов защиты информации в компьютерных системах; иметь практический опыт применения современных информационны х технологий и программных средств, в том числе отечественного	Лабораторн ая работа

		производства, при решении задач профессиональной деятельности	задач профессиональной деятельности	при решении задач профессиональной деятельности	средств, в том числе отечественного производства, при решении задач профессиональной деятельности	производства, при решении задач профессиональной деятельности	

2. Оценочные средства, необходимые для оценки результатов обучения по дисциплине (модулю)

Задания для устного опроса

Задания для устного опроса предназначены для оценки уровня сформированности компетенции УК-2
(индикатор достижения компетенции УК-2.1).

Тема 1. Основные понятия теории информационной безопасности
1. Какие методы защиты информации, использовавшиеся
в древнее время и в Средние века Вам известны?
2. Покажите связь между уровнем развития общества и технологиями защиты нформации.
3. В каких направлениях идет развитие теории информационной безопасности в настоящее время?
4. Каков вклад российских ученых в теорию информационной безопасности?
5. С чем связан возросший интерес к проблемам защиты информации?
6. Каковы отличия формального и неформального подходов к проблемам защиты информации?
7. В чем, на Ваш взгляд, заключаются основные трудности обеспечения информационной безопасности в настоящее время?
8. Что такое информационная система? Телекоммуникационная система? Автоматизированная система?
9. Каковы правовые понятия в области защиты информации?
10. Что такое защита информации? Информационная безопасность?
11. Охарактеризуйте понятия, связанные с организацией защиты информации.
12. Каковы основные принципы построения систем защиты информации?
13. Что такое комплексный подход к обеспечению информационной безопасности?
14. Каковы основные задачи защиты информации?
15. Докажите, что приведенное множество функций защиты является полным.
16. Какова взаимосвязь различных средств защиты информации? Есть ли среди них приоритетные?
17. Каковы основные средства реализации комплексной системы защиты информации?
18. Что такое морально-этические средства защиты информации?
19. Докажите необходимость сочетания различных средств
защиты информации.
20. Приведите примеры формальных и неформальных
средств защиты?
21. Что такое центры информационной безопасности и какова их роль в развитии теории и практики защиты информации?

Тема 2. Информация как объект защиты
1. Что такое информация и каковы уровни ее представления?
2. Перечислите основные носители информации, особенности их использования и защиты.
3. Какими свойствами определяется ценность информации?

4. Какие критерии оценки ценности информации Вы можете предложить?
5. Приведите примеры различной зависимости ценности информации от времени.
6. Что понимается под информационными ресурсами?
7. Что не разрешается относить к информации ограниченного доступа?
8. Что понимается под конфиденциальной информацией?
9. Какие существуют виды тайны?
10. Какое назначение имеет перечень конфиденциальных сведений предприятия?

Тема 3. Государственная политика информационной безопасности. Концепция комплексного обеспечения информационной безопасности

1. Каково место информационной безопасности в системе национальной безопасности Российской Федерации?
2. Сформулируйте основные положения Доктрины информационной безопасности РФ.
3. Каковы основные цели защиты информации?
4. Каковы основные задачи в области информационной безопасности?
5. Какова структура государственной системы защиты информации?
6. Кто несет ответственность за нарушение режима защиты информации?
7. Каковы функции руководителей предприятий при организации защиты информации?
8. Каковы основные функции ФСТЭК?
9. Покажите роль различных министерств и ведомств в вопросах защиты информации.

Тема 4. Угрозы информационной безопасности

1. На примере нескольких различных угроз покажите, что их осуществление приведет к изменению одного из основных свойств защищаемой информации (конфиденциальности, целостности, доступности).
2. Приведите примеры систем, для которых наибольшую угрозу безопасности представляет нарушение конфиденциальности информации.
3. Для каких систем (приведите примеры) наибольшую опасность представляет нарушение целостности информации?
4. В каких системах на первом месте стоит обеспечение доступности информации?
5. В чем различие понятий «нарушение конфиденциальности информации», «несанкционированный доступ к информации», «утечка информации»?
6. Определите перечень основных угроз для АС, состоящей из автономно работающего компьютера без выхода в сеть, расположенной в одной из лабораторий университета.
7. Постройте неформальную модель нарушителя для учебной компьютерной лаборатории.
8. Выведите формулу для расчета прочности трехуровневой защитной оболочки.
9. Охарактеризуйте защитные оболочки и перечень преград, применяемые в учебной компьютерной лаборатории.

Задания для устного опроса предназначены для оценки уровня сформированности компетенции ОПК-4
(индикатор достижения компетенции ОПК-4.1).

Тема 5. Построение систем защиты от угрозы нарушения конфиденциальности
1. В чем отличие терминов «НСД» и «Нарушение конфиденциальности информации»?
2. Что понимается под утечкой информации?
3. Каким образом классифицируются каналы утечки информации?

4. Каким образом следует выбирать меры защиты конфиденциальности информации?
5. Дайте определение идентификации и аутентификации
пользователя. В чем разница между этими понятиями?
6. Перечислите основные способы аутентификации. Какой, на Ваш взгляд, является наиболее эффективным?
7. Какие основные методы контроля доступа используются в известных вам информационных системах? В чем
их достоинства и недостатки?
8. Почему аутентификация с использованием пароля считается в настоящее время ненадежной?
9. Каковы методы аутентификации с использованием предметов заданного типа? Назовите те, которые получили распространение в последнее время.
10. Дайте определение шифра и сформулируйте основные требования к нему.
11. Поясните, что понимается под совершенным шифром.
12. Почему большинство современных шифрограмм могут
быть однозначно дешифрованы?
13. Каким образом государство регулирует использование
средств крипозащиты?

Тема 6. Построение систем защиты от угрозы нарушения целостности информации и отказа доступа
1. Каковы способы контроля целостности потока сообщений?
2. Какие существуют способы контроля целостности сообщений при взаимном доверии сторон?
3. Как контролировать целостность сообщений при высоком уровне помех в каналах связи?
4. Как организован обмен документами, заверенными цифровой подписью?
5. В чем отличие и сходство обычной и цифровой подписей?
6. Какими принципами нужно руководствоваться для сохранения целостности данных при их обработке?
7. Почему проблемы контроля целостности данных относятся к проблемам информационной безопасности?
8. Что означает контроль целостности данных на уровне
содержания? Приведите примеры.
9. Как обеспечить целостность данных при их хранении?
10. Что такое надежность и чем отличается надежность аппаратуры от надежности программного обеспечения?
11. Следует ли различать защиту от случайных угроз и от действий злоумышленника при

обеспечении беспрепятственного доступа к информации? Обоснуйте свой ответ.
12. Как защитить программное обеспечение от изучения логики его работы?
13. Предложите меры по обеспечению более надежной работы ЛВС университета.
14. Как изменяется надежность аппаратуры с течением времени?
15. Каковы способы повышения надежности аппаратуры
и линий связи?

Тема 7. Политика и модели безопасности
1. Что такое политика безопасности, кто ее разрабатывает
и где она применяется?
2. Приведите классификацию моделей разграничения доступа. Какова их роль в теории информационной безопасности?
3. Каковы основные достоинства и недостатки дискреционных моделей?
4. Приведите примеры использования дискреционных моделей разграничения доступа.
5. Составьте матрицу доступа и граф доступа для организации документооборота факультета (объекты доступа:
экзаменационные ведомости, персональные данные студентов, рабочие программы дисциплин; субъекты доступа: студенты, преподаватели, декан).
6. Что такое монитор безопасности и какие требования
к нему предъявляются?

7. Перечислите основные положения субъектно-объектного подхода к разграничению доступа? В чем достоинства и недостатки такого подхода?
8. В чем суть мандатной политики разграничения доступа?
9. Каковы основные достоинства и недостатки мандатной
политики?
10. Что такое скрытые каналы утечки информации и как их
обнаружить?
11. Почему ролевая политика получила большое распространение?
12. В чем суть моделей группового доступа?
13. Что такое информационная невыводимость и информационное невмешательство?
14. Как и зачем строятся многоуровненвые схемы разграничения доступа. Приведите пример.

Тема 8. Обзор международных стандартов информационной безопасности
1. Цели применения стандартов информационной безопасности.
2. Охарактеризуйте основные положения Оранжевой книги.
3. Почему в современных стандартах отказываются от единых шкал, характеризующих уровень безопасности?
4. Каковы основные положения Европейских критериев
безопасности информационных технологий?
5. Чем отличаются «информационная система» и «продукт
информационных технологий»?
6. Для чего вводятся критерии адекватности?
7. Что такое Профиль защиты?
8. В чем особенности Канадских критериев безопасности
компьютерных систем?

9. Опишите структуру Общих критериев безопасности информационных технологий.
10. Опишите технологию применения Общих критериев безопасности информационных технологий.
11. Каковы тенденции развития международной нормативной базы в области информационной безопасности?

Критерии оценки (в баллах)

- *1 балл выставляется студенту, если он отвечает на предложенный вопрос;*
- *0 баллов выставляется студенту, если он не отвечает на предложенный вопрос.*

Тестовые задания

Тестовые задания предназначены для оценки уровня сформированности компетенции УК-2 (индикатор достижения компетенции УК-2.2).

1. Установите верное соответствие видов информации с их содержательным определением

- А. Документированная информация
- Б. Электронный документ
- В. Данные

1) информация, представленная в виде, пригодном для обработки автоматическими средствами при возможном участии человека
2) зафиксированная на материальном носителе путем документирования информация с определенными реквизитами
3) документированная информация, представленная в виде, пригодном для восприятия человеком с использованием электронных вычислительных машин.

2. Переводчик, согласно федеральному закону «Об информации, информационных технологиях и о защите информации», при отсутствии иных условий, может рассматриваться в качестве обладателя

1) Текста переводимого им произведения
2) Используемого им в работе словаря
3) Созданного им перевода текста
4) Документа с замечаниями редактора к созданному переводу

3. Предоставление информации отличается от распространения информации, согласно федеральному закону «Об информации, информационных технологиях и о защите информации»

1) Характером лица или круга лиц, осуществляющего получение информации
2) Стороной, являющейся инициатором действий
3) Характером лица или круга лиц, осуществляющего передачу информации

4) Формой представления передаваемой информации
5) Конфиденциальностью передаваемой информации
6) Количеством лиц, осуществляющих получение информации

4. Укажите все ситуации, которые, согласно федеральному закону «Об информации, информационных технологиях и о защите информации», можно рассматривать как распространение информации:

1) Публикация статьи в средствах массовой информации
2) Рассылка внутреннего регламента сотрудникам организации на основе штатного расписания по корпоративной почте
3) Размещение бумажного объявления на доске объявлений
4) Демонстрация презентации на совещании руководителей отделов
5) Демонстрация учебного видео на уроке в школе
6) Размещение записи на странице в социальной сети

5. Согласно федеральному закону «Об информации, информационных технологиях и о защите информации», электронный документ - документированная информация, представленная в электронной форме, то есть в виде, пригодном для восприятия:

1) Человеком с использованием электронных вычислительных машин
2) Техническими средствами информационных систем
3) Программным обеспечением информационных систем
4) Программным обеспечением систем обработки информации

6. Автоматизированная система, согласно ГОСТ «Информационная технология. Комплекс стандартов на автоматизированные системы. Автоматизированные системы. Термины и определения», состоит из

1) Информации и средств автоматизации ее обработки
2) Персонала и комплекса средств автоматизации его деятельности
3) Информационной технологии и средств автоматизации ее осуществления
4) Установленных функций персонала и средств автоматизации их выполнения

7. Защищаемая информация, согласно ГОСТ «Защита информации. Основные термины и определения» - это подлежащая защите информация,

1) Не являющаяся общеизвестной
2) Представляющая ценность для ее обладателя
3) Являющаяся предметом собственности
4) Относящаяся к установленной законом категории

8. Укажите все варианты того, что может являться объектом защиты информации, предусмотренные ГОСТ «Защита информации. Основные термины и определения»:

1) Информация
2) Носитель информации
3) Система обработки информации
4) Информационная технология
5) Информационный процесс

Тестовые задания предназначены для оценки уровня сформированности компетенции ОПК-4 (индикатор достижения компетенции ОПК-4.2).

1. Укажите все мероприятия, направленные на обеспечение конфиденциальности информации:

1) Установка паролей для доступа к электронным документам
2) Создание резервных копий важных файлов
3) Контроль изменений, вносимых в важную информацию легальными пользователями
4) Контроль надежности работы оборудования информационной системы
5) Установка запрета на запись служебных документов на съемные носители информации
6) Уничтожение носителей важной информации при помощи специального оборудования

2. Укажите все мероприятия, направленные на обеспечение целостности информации:

1) Ведение журнала регистрации изменений, внесенных в базу данных зарегистрированными пользователями
2) Использование надежных носителей информации, замена при истечении гарантийного срока
3) Проведение профилактических работ с оборудованием информационной системы
4) Ограничение прав пользователей на запись в важные файлы
5) Запрет отправки определенных документов по электронной почте

3. К видам информации, защищаемой законодательством РФ, относятся (выберите несколько вариантов):

a. персональные данные;

b. служебная тайна;

c. список кандидатов на выборы в Госдуму;

d. справочная информация организации.

4. Установите соответствие между понятиями и их определениями:

А1. Информационные продукты – это…	А2. …стоимостная категория информации, характеризующая конкретный размер прибыли при ее использовании или размер убытков при ее утрате.
Б1. Ценность информации – это…	Б2. … действия субъектов (собственников и владельцев ресурсов) по обеспечению пользователей информационными продуктами.
В1. Информационная услуга – это…	В2. … документированная информация, подготовленная в соответствии с потребностями пользователей и предназначенная или применяемая для удовлетворения потребностей пользователей.

5. Закончите определение: лицо, действующее в интересах конкурента, противника или в личных корыстных интересах (агентов иностранных спецслужб, промышленного и экономического шпионажа, криминальных структур, отдельных преступных элементов, лиц, сотрудничающих со злоумышленниками, психически больных и пр.), называется …

6. Если пользователи создают свои собственные пароли, каких рекомендаций они должны придерживаться (выберите все возможные варианты)?

a. использовать максимально возможное количество символов в пароле;

b. использовать в качестве пароля имя супруга/супруги, ребенка или кличку собаки (чтобы не забыть пароль);

c. использовать хотя бы одну прописную букву, один символ нижнего регистра, одну цифру и один допустимый не алфавитно-цифровой символ;

d. использовать пароль, который трудно угадать по смыслу.

7. Напишите развернутый ответ на вопрос: что, на ваш взгляд, является информационно-аналитической работой?

Критерии оценки (в баллах) каждого тестового задания:

- *1 балл выставляется студенту, если он правильно выполняет тестовое задание;*
- *0 баллов выставляется студенту, если задание не выполнено или решено неверно*.

Задания для лабораторных работ

Задания для практических работ предназначены для оценки уровня сформированности компетенции ОПК-4 (индикатор достижения компетенции ОПК-4.3).

Лабораторная работа №1.

Задание: Разработать доклад на тему в соответствии с вариантом. Подготовить слайды и сделать презентацию доклада.

Варианты:

1. Основные понятия информационной безопасности. Угрозы и меры противодействия
2. Классификация угроз безопасности информации в компьютерных системах

3. Информационная безопасность в сети Интернет
4. Информационная безопасность Интернета вещей.
5. Программно-технические способы и средства обеспечения информационной безопасности
6. Организационная защита объектов информатизации
7. Информационная безопасность предприятия
8. Нормативные документы в области информационной безопасности
9. Органы (подразделения), обеспечивающие информационную безопасность
10. Криптографические методы защиты информации
11. Компьютерные вирусы и механизмы борьбы с ними
12. Защита информации в распределенных компьютерных системах
13. Информационная безопасность в повседневной жизни
14. Безопасность личности в информационном обществе
15. Комплексные системы защиты информации в компьютерных системах
16. Тенденции в области индустрии информационной безопасности. Перспективы развития
17. Политика информационной безопасности
18. Информационная безопасность в экономической сфере

Лабораторная работа №2.

Задание: Подготовьте файл с таблицей для анализа законодательных актов из приведенного ниже списка. В таблице отразите такие параметры, как название законодательного акта, понятия, объекты, цели, основные положения. Выберите не менее пяти, наиболее важных на ваш взгляд, законодательных актов и заполните таблицу.

Лабораторная работа №3.

Задание: Написать компьютерную программу, реализующую аналитический метод шифрования на основе следующих матричных преобразований. Ключом в алгоритме является заданная обратимая квадратная матрица. Этап зашифровывания: вектор с числовыми кодами (порядковыми номерами букв в алфавите) символов шифруемого текстового сообщения умножается на матрицу-ключ, в результате произведения получается числовой вектор шифр-текста. Этап расшифровывания: вычисление решения СЛАУ, где основная матрица – ключ алгоритма шифрования, а правый столбец – вектор шифр-текста; результатом решения СЛАУ является вектор, состоящий из порядковых номеров букв русского алфавита. Для точного решения СЛАУ и как следствие однозначного сопоставления вычисленного вектора решения с буквами в алфавите, разработать и использовать класс для работы с обыкновенными дробями с перегруженными арифметическими операциями.

С помощью разработанной программы:

1) Зашифровать свои ФИО на основе произвольно выбранного ключа;

2) Для заданного ключа расшифровать сообщение, указанное в варианте.

Варианты:

№	Шифр-код
1	11 35 42 16 26 11 33 16 35 36 24 12 11 13 24 42 13 16 26 11
2	23 34 31 34 42 55 16 36 43 26 24 23 11 41 16 36 16 12 36 34 33 16 26 43 35 24 52 56
3	34 42 14 31 43 35 34 14 34 36 24 41 26 11 15 34 12 16 15 55 12 31 24 23 26 34
4	35 36 24 13 63 23 11 33 33 34 14 34 31 56 13 11 24 23 11 25 46 55 31 63 14 11 62 42
5	35 43 41 42 11 63 32 16 31 56 33 24 46 11 24 12 16 23 13 16 42 36 11 32 16 31 16 42
6	23 11 15 43 32 11 31 12 16 22 11 42 56 42 11 26 33 16 51 16 14 34 31 16 22 11 42 56
7	35 34 15 11 31 56 52 16 34 42 46 11 36 16 25 14 34 31 34 13 11 46 16 31 16 25
8	43 16 22 11 34 15 33 11 41 24 31 11 26 34 31 62 51 26 24
9	12 43 26 13 55 26 36 24 13 55 16 15 11 41 32 55 41 31 35 36 63 32 34 25
10	35 34 36 34 22 33 24 25 26 34 31 34 41 13 55 52 16 41 42 34 24 42
11	31 11 41 26 34 13 34 16 41 31 34 13 34 35 43 53 16 15 43 12 24 33 55
12	31 43 51 52 16 43 51 16 33 55 25 51 16 32 23 34 31 34 51 16 33 55 25
13	26 33 24 14 11 26 33 24 14 34 25 11 32 34 23 14 11 32 24 15 13 24 14 11 25
14	41 55 42 34 16 12 36 62 45 34 26 43 51 16 33 24 62 14 31 43 45 34
15	41 34 12 11 51 56 63 15 36 43 22 12 11 15 34 35 16 36 13 34 25 26 34 41 42 24

Лабораторная работа №4.

Задание: Написать компьютерную программу, реализующую алгоритм шифрования RSA.

С помощью разработанной программы:

1) Зашифровать свои ФИО на основе произвольно выбранного ключа;

2) Для заданного ключа расшифровать сообщение, указанное в варианте.

Критерии оценки (в баллах)

5-7 – баллов выставляется студенту, если он правильно выполняет задание, демонстрирует его решение и отвечает на дополнительные вопросы;

3-4 – баллов выставляется студенту, если он правильно выполняет задание и отвечает на дополнительные вопросы;

1-2 – баллов выставляется студенту, если он выполняет задание при помощи наводящих вопросов и/или не отвечает на дополнительные вопросы;

0 – баллов выставляется студенту, если он не может выполнить задание и ответить на дополнительные вопросы.

Задания для контрольных работ

Задания для контрольной работы предназначены для оценки уровня сформированности компетенции УК-2 (индикатор достижения компетенции УК-2.3).

Описание контрольной работы №1:

Контрольная работа представляет собой письменное задание, рассчитанное на выполнение в течение 90 минут, и включает в себя ответы на 5 теоретических вопросов.

Типовой вариант контрольной работы

1. Дайте определение терминам: конфиденциальность, целостность и доступность информации.
2. Охарактеризуйте известные вам методам аутентификации.
3. Перечислите способы контроля целостности сообщений при взаимном доверии сторон.
4. Приведите примеры мероприятий, направленные на обеспечение целостности информации.
5. Дайте развернутый ответ на вопрос «Чем отличается предоставление информации от распространения информации, согласно федеральному закону «Об информации, информационных технологиях и о защите информации»?

Описание контрольной работы №2:

Контрольная работа представляет собой письменное выполнение 10 заданий.

Задание 1. Шифр атбаш

Шифры появились в глубокой древности в виде криптограмм (по-гречески — тайнопись). Священные иудейские тексты шифровались методом замены. Вместо первой буквы алфавита записывалась последняя буква, вместо второй — предпоследняя и т. д. Этот древний шифр назывался **атбаш**.

А	Б	В	Г	Д	Е	Ё	Ж	З	И	Й	К	Л	М	Н	О	П	Р	С	Т	У	Ф	Х	Ц	Ч	Ш	Щ	Ъ	Ы	Ь	Э	Ю	Я
я	ю	э	ь	ы	ъ	щ	ш	ч	ц	х	ф	у	т	с	р	п	о	н	м	л	к	й	и	з	ж	ё	е	д	г	в	б	а

Пример выполнения

Исходный текст: «ВРАГ»

Зашифрованный текст «ЭОЯЬ»

1. Зашифровать свою фамилию, имя и отчество с помощью шифра **атбаш**.
2. Дешифровать сообщение, зашифрованное с помощью шифра **атбаш**

Вар	**Шифрограмма (шифр атбаш)**
1	ЭФЯШЫРХЫЪНАМФЪЪНМГНЭРХСРУГ
2	ЧЛЮДТЛЫОРНМЦПРАЭУАБМНАЧСЯЗЦМЪУГСРПРЧШЪФУДФРЭ
3	ФМРТЪЖЯЪММЪЮЪЭДЫЛТЯМГПРОРЙСЪПОРТРФЯЪТДХ
4	СЪЭРЭНАФРХЦЬОЪМЛЧДЭДЦЬОДЭЯБМ
5	МЯФЙРЗЪМНАЮДМГСЛШСДТСЛШСДТУБЫАТ
6	СЯНЛЖЪТСРЬРЛТСДЙФРЬЫЯСЯТРОЪЮЪЫЯ
7	СЪМСЛШЫДЭЪЖЯМГФРУРФРУГЗЦФСЯЫЛОЯФЯ
8	КЦУРНРКНФЦХЭЧЬУАЫСЯЭЪЁЦПРЧЭРУАЪМРЮЙРЫЦМГНАЮЪЧСЦЙ
9	ЭНЪПРЮЪЫДСЯЗЦСЯБМНАНПРЮЪЫСЯЫНЯТЦТНРЮРХ
10	СЯЛФЯСЪПРЬОЪЖЦТЯСРЛЗЪСДЪПРНМРАССРРЖЦЮЯБМНА
11	ПЯОЯЫРФНВМРЦНМЦСЯЪЁЩСЪНМЯЭЖЯАЮЯСЯУГСРНМГБ
12	УЪФЯОНМЭРСЪЫРУШСРЮДМГЙЛШЪНЯТРХЮРУЪЧСЦ
13	КРОМЛСЯЗЯЁЪЭНЪЬРЛУДЮЯЪМНАМРТЛФРЬРСЪЧЯТЪЗЯЪМКЪТЦЫЯ
14	НРЖЪЫЖЪТЛНПГЪЫЪНМЯУЯМОЛЫСРТЪСАМГПРЧЛ
15	ФЯШЫДХНРРЮЁЯБЁЦХНАНРНЛЫЛЭЪОЪСЗМРЪЬРЛОРЭЪСГЭДЖЪ

Задание 2. Шифр Цезаря

Известен факт шифрования переписки Юлия Цезаря с Цицероном. **Шифр Цезаря** реализуется заменой каждой буквы в сообщении другой буквой этого же алфавита, отстоящей от нее в алфавите на фиксированное число букв. В своих шифровках Цезарь заменял букву исходного открытого текста буквой, отстоящей от исходной буквы впереди на три позиции.

Пример выполнения

Исходный текст: «КОЗИНА ГАЛИНА ЛЕОНИДОВНА»

Используем алфавит, содержащий 33 буквы и пробел, стоящий после буквы Я:

АБВГДЕЁЖЗИЙКЛМНОПРСТУФХЦЧШЩЪЫЬЭЮЯпробел

Ключом в шифре Цезаря является число 3. Каждая буква в исходном тексте сдвигается по алфавиту на 3 позиции. Таким образом, получаем:

Исходный текст	КОЗИНА		ГАЛИНА		ЛЕОНИДОВНА
Зашифрованный текст	НСКЛРГ	В	ЁГОЛРГ	В	ОЗСРЛЖСЕРГ

1. Зашифровать свою фамилию, имя и отчество с помощью шифра **Цезаря**.
2. Дешифровать сообщение, зашифрованное шифром **Цезаря**.

Вар	**Шифрограмма (шифр Цезаря)**
1	ТСДЗЖЛХЗОЯОБДЛХТУЗЦЕЗОЛЪЛЕГХЯФЛОЦТСДЗЙЖЗРРСЁС
2	ЪЗПШЦЙЗРСЕСФХЯХЗПДСОЯЫЗЛРЧСУПГЩЛЛСРГФСЖЗУЙЛХ
3	ТУГЕЛОГЖОВЕФЗШСЖЛРГНСЕЮЗХСОЯНСЛФНОБЪЗРЛВУГКРЮЗ
4	ЛКСДУЗХГХЗОВНСОЗФГСФСДЗРРСЪХВХДЗОНЛ
5	ДЗФТУЛРЩЛТРСФХЯАХСРЗСХФХЦХФХЕЛЗТУЛРЩЛТСЕГЛШЛКСДЛОЛЗ
6	НГНПГОССНУЮОЗРРЮШФУЗЖЛСНСОЯЩСЕГРРЮШ
7	НХСЕФЗЁЖГФЛЖЛХРГПЗОЛХСХРЛНСЁЖГРЗЦХСРЗХ
8	ХСХЙЛЕЗХТУЛТЗЕГБЪЛНХСЙЛЕЗХТСЖТЗЕГБЪЛ
9	ТУЗЙЖЗЪЗПЕЮШСЖЛХЯЛКФЗДВСТУЗЖЗОЛХЗЖГОЯРЗМЫЛМПГУЫУЦХ
10	СУОЮФЛЖВХОЛДСРГЕЗУЫЛРЗОЛДСЕНОЗХНЗ
11	РГЦНЛДЮЕГБХЗФХЗФХЕЗРРЮПЛЛТУСХЛЕСЗФХЗФХЕЗРРЮПЛ
12	ВЛФГПЫЦХЛХЯРЗОБДОБЛОБЖВПРЗЖГП
13	ЗФОЛДГУЛРДЗКФГТСЁКРГЪЛХДГУЛРТЗЖГЁСЁ
14	ЛПЗБЬЛМЦЫЛЖГРЗСФХГРЗХФВДЗКОГТЫЛ
15	КГУВЙЗРРСПЦХГРНЦЕЖЦОСРЗФПСХУВХ

Задание 3. Квадрат Полибия 6 × 6

В Древней Греции (II в. до н.э.) был известен шифр, который создавался с помощью **квадрата Полибия**. Таблица для шифрования представляла собой квадрат с 5 столбцами и 5 строками, которые нумеровались цифрами от 1 до 5. В каждую клетку такой таблицы записывалась одна буква. В результате каждой букве соответствовала пара цифр, и шифрование сводилось к замене буквы парой цифр.

Пример выполнения

Число букв в русском алфавите отличается от числа букв в греческом алфавите, поэтому и размер таблицы выбран иным (квадрат 6 × 6). Порядок расположения символов в квадрате является секретной информацией (ключом).

	1	2	3	4	5	6
1	**А**	**Б**	**В**	**Г**	**Д**	**Е**
2	**Ё**	**Ж**	**З**	**И**	**Й**	**К**
3	**Л**	**М**	**Н**	**О**	**П**	**Р**
4	**С**	**Т**	**У**	**Ф**	**Х**	**Ц**
5	**Ч**	**Ш**	**Щ**	**Ъ**	**Ы**	**Ь**
6	**Э**	**Ю**	**Я**	**,**	**.**	**-**

Зашифруем с помощью квадрата Полибия слово КРИПТОГРАФИЯ:

26 36 24 35 42 34 14 36 11 44 24 63

Из примера видно, что в шифрограмме первым указывается номер строки, а вторым – номер столбца. В квадрате Полибия столбцы и строки можно маркировать не только цифрами, но и буквами.

1. Зашифровать свою фамилию, имя и отчество с помощью квадрата **Полибия** 6×6.
2. Дешифровать сообщение, зашифрованное с помощью квадрата **Полибия** 6×6.

Вар	**Шифрограмма (квадрат Полибия)**
1	11 35 42 16 26 11 33 16 35 36 24 12 11 13 24 42 13 16 26 11
2	23 34 31 34 42 55 16 36 43 26 24 23 11 41 16 36 16 12 36 34 33 16 26 43 35 24 52 56
3	34 42 14 31 43 35 34 14 34 36 24 41 26 11 15 34 12 16 15 55 12 31 24 23 26 34
4	35 36 24 13 63 23 11 33 33 34 14 34 31 56 13 11 24 23 11 25 46 55 31 63 14 11 62 42
5	35 43 41 42 11 63 32 16 31 56 33 24 46 11 24 12 16 23 13 16 42 36 11 32 16 31 16 42
6	23 11 15 43 32 11 31 12 16 22 11 42 56 42 11 26 33 16 51 16 14 34 31 16 22 11 42 56
7	35 34 15 11 31 56 52 16 34 42 46 11 36 16 25 14 34 31 34 13 11 46 16 31 16 25
8	43 16 22 11 34 15 33 11 41 24 31 11 26 34 31 62 51 26 24
9	12 43 26 13 55 26 36 24 13 55 16 15 11 41 32 55 41 31 35 36 63 32 34 25
10	35 34 36 34 22 33 24 25 26 34 31 34 41 13 55 52 16 41 42 34 24 42
11	31 11 41 26 34 13 34 16 41 31 34 13 34 35 43 53 16 15 43 12 24 33 55
12	31 43 51 52 16 43 51 16 33 55 25 51 16 32 23 34 31 34 51 16 33 55 25
13	26 33 24 14 11 26 33 24 14 34 25 11 32 34 23 14 11 32 24 15 13 24 14 11 25
14	41 55 42 34 16 12 36 62 45 34 26 43 51 16 33 24 62 14 31 43 45 34
15	41 34 12 11 51 56 63 15 36 43 22 12 11 15 34 35 16 36 13 34 25 26 34 41 42 24

Задание 4. Таблица Виженера

Это шифр представляет шифр Цезаря с переменной величиной сдвига. Величину сдвига задают ключевым словом. Зашифрование заключается в том, что первый из алфавитов соответствует алфавиту открытого текста, а букве ключевого слова соответствует алфавит шифрования из данного списка, начинающийся с этой буквы. Буква шифрованного текста находится в алфавите шифрования на месте, соответствующем данной букве открытого текста.

Пример выполнения

Ключ «ДАР». Исходный текст «КОЛБА». Зашифрованный текст «ЖОЫЭА»

	А	**Б**	**В**	**Г**	**Д**	**Е**	**Ё**	**Ж**	**З**	**И**	**Й**	**К**	**Л**	**М**	**Н**	**О**	**П**	**Р**	**С**	**Т**	**У**	**Ф**	**Х**	**Ц**	**Ч**	**Ш**	**Щ**	**Ъ**	**Ы**	**Ь**	**Э**	**Ю**	**Я**
Д	Ь	Э	Ю	Я	А	Б	В	Г	Д	Е	Ё	Ж	З	И	Й	К	Л	М	Н	О	П	Р	С	Т	У	Ф	Х	Ц	Ч	Ш	Щ	Ъ	Ы
А	А	Б	В	Г	Д	Е	Ё	Ж	З	И	Й	К	Л	М	Н	О	П	Р	С	Т	У	Ф	Х	Ц	Ч	Ш	Щ	Ъ	Ы	Ь	Э	Ю	Я
Р	П	Р	С	Т	У	Ф	Х	Ц	Ч	Ш	Щ	Ъ	Ы	Ь	Э	Ю	Я	А	Б	В	Г	Д	Е	Ё	Ж	З	И	Й	К	Л	М	Н	О
Д	Ь	Э	Ю	Я	А	Б	В	Г	Д	Е	Ё	Ж	З	И	Й	К	Л	М	Н	О	П	Р	С	Т	У	Ф	Х	Ц	Ч	Ш	Щ	Ъ	Ы
А	А	Б	В	Г	Д	Е	Ё	Ж	З	И	Й	К	Л	М	Н	О	П	Р	С	Т	У	Ф	Х	Ц	Ч	Ш	Щ	Ъ	Ы	Ь	Э	Ю	Я

1. Зашифровать свою фамилию, имя и отчество с помощью таблицы **Виженера** (см. Приложение А). В качестве ключа использовать свое имя.
2. Дешифровать сообщение, зашифрованное с помощью таблицы **Виженера**.

Вар	**Ключ**	**Шифрограмма (Таблица Виженера)**
1	ОБИЛЬНО	ХНШЕТЁЯМКЁЭЛТЯЕГГЭЁБЪБНИЖСНЫУЗЫЭЩБХЪС ШГОБЮСЖГГТУЪЭЫЕГМВВЪЦКШПЫУАРЁЦОЁГАЛЯ ФУТЖАЛАЁТЭАЮ
2	ТУПИК	АОЯЗМТЮГЩИЭЫЬЬЭЫЗГКЕЪЧЭШДЩХЩШЪЯЮЩГ ЮМЫЧЁШЮМШКВБХВЙЁНВДЩДЭЭХВЮСАИКЧИЪД ЮЩНКГЕХЭЭЛЮДШ
3	НИТКА	ЭЗЬЩИАЬЩУББЩЙИНТИПЮЗУТАААЕЕЬЭБИЕИМИКТ ЮСДГБЩРЁУЦАЩИЧКЬЪРПГЁЭСЕЯЬУЩОАААААИАЁП ЁАХКПДБЫЫБГЕЦЧСЮМ
4	ДРУЗЬЯ	ЙШОЪИССЭСЫПАААОЪЬЁРБАСЬХЙГГЮЬФФДЛЛЕМСЬ ЧПБПЭАОЛЕМЙЙПЬДИГЬВИЁДНУЛЛЩИСБВОЩТСШР СЕИСДПООИЬНЭСЫТЕЫОЩБ
5	ЖИЗНЬ	ЖЧРВЧЛУБЪСВЁКЭЧЭЧЪАМДКЬТЦЩВЖЧОЙЧКЭТКЗ ЖЙСЗЬЙБЕФЙБЧЫЛЁЯЫЛЖАЖДЦЩЬКДГЕАРОЫЮЗК ТРЮЮЬТЦЩДБВФВШУЕМШКЩНЦВЦ
6	ФРЕГАТ	ФЧЖВТЫЛУАДДНШШЬЛГНЮКРКАПЭВЛВЧБНФННУЦ НЮЖКЕЪЖСЦМЛИНПАЙННАААААЛЕЫБОЭЧКЭЭЕЪ ЩПЬНЕПЩФ
7	ЗВЕЗДЫ	КЮЖШЙЧЛЛДГУЙЕСТБЙАБНЙЙОЙЫМДЁОЙИГМЛБЧ ЙМЖФЕЦЛРЧШОЙГРЙЁБЪЪЮНШБЧЙЛАЩЬМЪГГЬНЧ ШОЫЦОЦЧЛЫЪБЭШРЧБСТШБЛЛАБ
8	СТРУНА	РЯФНСВЭПЭАЕРККЯЫЗИАЬЫИФПЧАПОЫЧВПБЯФУН ЯЪОБЗКЯВСАЫЮЬМЯАЕРЮПДБНБЬЫИЭОПЬЫИДТЯБ ЭМЫНУЮСХВРВАПЪЕЕЬЫК
9	СВЕЧА	ААЙЙОТЮШЫОЮООЫКОРЩЬСРОРЧЪДВЦЙЖЛЧЦЧЪО РГНЬЯАЪЙШЛОРААТЭЛЫХЛМЯДЫЬЦЮТЫОЬЮЗЬМЧ ОЫЫЬЬЮТЫОААЙЖСРГТЬНУЧЫМНЭРЛИТЧРЧ
10	ПОМПЕЯ	ЮЪЕЫЙММЬВАЛПЗЪИЮАДЬЕГХАГВЦЁХЁУЯУФДЯО ЩИБЯЗВХЩЖЭДЙАВШЫЛБВЯВАЙНЮРВАЙНАЦШЯК АГНЕХЖЙЬЪЕМИБТЦЫДЭЙЩ
11	СВОБОДА	ЮОЪБМУНЙГТДЩИОЪАГСУПЮБЛСПААЫПГЩЖУПЧ ЬЩЦВАМЛОЛРСББТВУЪЛМНОЦВСММАЛНПИЯГОЬН ЖГБАЭОТЩЬЯЬМЫПЮХКРЛОЪГДЯЪПХЧ
12	ЗАПРЕТ	ПТЯРЭИЯИГЛДЭИОЧШНЙЁАНВЙЪЙВХВАЭЖКРЧАЪД ЯЮФМПБХЮГННЙОВШЯТИЖЩБАОЧНРВЛЬВСГСАЫ ЁОЭЧЫЭИЕГФИТЩОЪЬЪЫЭНРУАЧЙЯЮФКЮЖСЩ
13	КАРТЫ	КОВМНЖЛПСУЖТФЫЕЭАААФДСАНМИДСБСЮДВЦИ ДРЮРЕВНФЩБЭЯЮСТДЙЪЬРДДЮЧПХРВЦЗЁАВЙНЖ ДЛМЖДЛЮЪНЖБЮРУВ
14	РАЗЛУКА	ФСДЭЭЧЕВСЧЧШИБЮКШУЮЧЯЧЬЩГШСРП ЗИПОХВААПЗСЗСОСЖАИУХЮРЖМЫЁАБСК ФОХТЛСЧЁЩЪЯБЬЁФРЖОРОВВМЩРПЗДЗЧД ЙЭАЬХЫБЬН
15	НАУКА	СОВБАЦЕШАНТУДГЫЯКЪЮЖЭАЩГЕВОЯДМЁЧЯДБН ЛШЪНЫВАМЕАЬЛАОГЕЪСГБРСАСЮИЕАОЯАЬБОЦКМ

		АПГАОЮЛБЧСЁВЫВ

Задание 5. Метод перестановок

В шифре **перестановок** все буквы открытого текста остаются без изменений, но перемещаются с их исходных позиций на другие места (примером является шифрование с помощью скиталы).

Следующая простейшая «шифровка» получена методом перестановки двух соседних букв РКПИОТРГФАЯИ. В этом «секретном» сообщении легко узнать слово КРИПТОГРАФИЯ.

Более сложный алгоритм перестановок сводится к разбиению сообщения на группы по три буквы. В каждой группе первую букву ставят на третье место, а вторую и третью буквы смещают на одну позицию влево. В результате получится криптограмма: РИКТОПРАГИЯФ.

Перестановки получаются в результате записи исходного текста и чтения шифрованного текста по разным путям некоторой геометрической фигуры.

1. Зашифровать фрагмент стихотворения (64 символа) методом **перестановок**. Ключ и текст выбрать самостоятельно. Записываем построчно в матрицу-квадрат шифрограмму, затем упорядочиваем построчно по ключу считывания, затем упорядочиваем по столбцам по ключу записи.
2. Дешифровать сообщение, зашифрованное методом **перестановок**.

Вар	**Мат-рица**	**Ключ записи**	**Ключ считывания**	**Шифрограмма**
1	10x10	8 2 5 4 1 3 7 9 6 10	1 9 3 8 5 4 7 2 6 10	ППОЕСИЛУЧООЧИТСЗГОВ6ОЛНЛАНЧ ОО1ГАЯККЕОПО7ТЛЮИОНОЕО2ОИУО ЛИУСД9ЕДЬААВТАГ4ЛАЛТТЗАСТ3ЧИС ТТЕТДЛ8ВУПЕВЛОДЖ5
2	10x10	10 1 2 3 9 4 8 5 7 6	10 1 2 3 6 4 5 7 9 8	НСОЕХ1ИНКИМИЯ_Е_НГВПИЯ_ОР1ЕО АО_ММТЕ9Т_РДРТЛУО8УБЕЛВИБЫ_Д9_ ТН_Ы_СКК8ДАЫСАААИР_7ХА_АЕТКЩА 4М_АКЖЯ_ЯП5АКТД
3	10x10	8 2 5 4 1 3 7 9 6 10	1 9 3 8 5 4 7 2 6 10	ДВРВОУМКГ8ИОИБА9ЙЛГ3ОКВАВИН ЖТ7ТРДИЧ1ЕЕЕ7ЛОСОТЬИЫВ6БКОКСТ ЯДО4СООНЕЯНЧН4ЬЕЕКЯЧЕАО3АТХЙ РСВЙУ5ПГТУЮ2ЯОО8
4	10x10	10 9 1 8 2 7 3 6 4 5	5 6 4 7 3 8 1 9 2 10	но_илиен_витряеяттинакинснлаьояоа_н_еа сав_теиепфнн_рсииинзсяд_неыж_окОэус_я зыил_овирчдв_астюув_м_яет
5	9x9	3 1 2 4 9 7 8 6 5	5 1 2 7 9 4 8 6 3	олоосахаопвГкЭеывор_ламтйылявтуньныу ___т7__анхопдрРикктуи__февмдосмол_з_и гуже__сь
6	9x9	1 2 3 8 7 6 9 5 4	1 9 4 2 8 7 6 5 3	Оо_1___моото5тптеоинс9нунчмдцн2пдпут дют6ю_юнтеао4аеа_чнвп7мимо__и_8игиту неа3оро_о
7	9x9	6 1 5 2 4 3 8 9 7	1 2 3 9 8 7 6 5 4	лн_в_Оотеиомоддвы___ызон_смл__ьчп_ж ниыутоайаонб_иткедироьда_д_летлутйючл ччсбсоляи
8	8x8	8 1 2 3 7 6 5 4	4 1 2 3 7 6 5 8	раооис_дм0ееянэВе_тт_ет_тсррм_оо1ии1и тем_т__лищоенввлчен0м_2ма__

9	10x10	10 9 1 8 2 7 3 6 4 5	10 9 1 8 2 7 3 6 4 5	еыьа8_лбдыррпв9евозралеслюхш_К_омо4н яроененуот_ебоятов5_опстымищ_еднымло кт3вп__ю__яе1роилпдк_с2о_яиь
10	9x9	2 1 4 3 6 5 7 8 9	8 9 6 7 4 5 3 2 1	сра_ошв17еслнвеа58итиеаыяу7сощвзс__6_ оацб_еа9дкщирв_д8хдзаооид3и__т_нн_4кЯ ере_ам2

Задание 6. Шифры "Пляшущие человечки"

Основной метод расшифровки подобных шифров - частотный анализ. (+ логические рассуждения).

Таблица частот:

В русском языке в каждой тысяче символов в среднем встречается

пробел	175	**р**	40	**я**	18	**х**	9
о	90	**в**	38	**з**	16	**ж**	7
е, ё	72	**л**	35	**ы**	16	**ш**	6
а	62	**к**	28	**б**	14	**ю**	6
и	62	**м**	26	**ъ, ь**	14	**ц**	4
н	53	**д**	25	**г**	13	**э**	3
т	53	**п**	23	**ч**	12	**щ**	3
с	45	**у**	21	**й**	10	**ф**	2

Чаще всего буквы заменяют другими буквами.

1. Зашифровать фрагмент стихотворения (64 символа) с помощью частотной таблицы.
2. Расшифровать текст:

Сзргйзю тсуцълн Уйиефнлм цкрго, ъхс зов кргнспфхег ф зиецынсм ргзс тсзсмхл, ритулрцйзиррс тсжсесулхя с тсжсзи л тсфои ахсжс туизфхгелхяфв. Рг сзрсм лк тусжцосн ср тсефхуиъго жцовбьцб ф дсосрнсм зиецынц. Тсуцълн тсзсыио н рим, трцо ии дсосрнц хгн, ъхс хг згоинс цоихиог л фнгкго:

- Рлкнс оихлх. Елзгхя, н зсйзб. Нфхгхл, угкуиылхи туизфхгелхяфв, тсуцълн Уйиефнлм.

Задание 7. Алгоритм шифрования ГОСТ 28147-89

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.

Пример выполнения

Исходные данные для зашифрования: КОЗИНА Г

Для ключа возьмем последовательность состоящую из 32 букв:

АЛИНа пошла в лес собирать грибы

Для первого подключа X используем первые 4 буквы ключа: АЛИН.

Переводим исходный текст и первый подключ в двоичную последовательность (см. Приложение Б):

исходный текст

К	11001010
О	11001110
З	11000111
И	11001000
Н	11001101
А	11000000
пробел	00100000
Г	11000011

первый подключ X0

А	11000000
Л	11001011
И	11001000
Н	11001101

Таким образом, первые 64 бита определяют входную последовательность

L0:	11001010	11001110	11000111	11001000
R0:	11001101	11000000	00100000	11000011

следующие 32 бита определяют первый подключ

X0:	11000000	11001011	11001000	11001101

I. Найдем значение функции преобразования f(R0,X0)

1). Вычисление суммы R0 и X0 по mod 2^{32}

R0:	1100 1101	1100 0000	0010 0000	1100 0011
X0:	1100 0000	1100 1011	1100 1000	1100 1101
	1000 1110	1000 1011	1110 1001	1001 0000

2). Преобразование в блоке подстановки

Результат суммирования R0+X0 по mod 2^{32}

1000 1110 1000 1011 1110 1001 1001 0000

преобразуем в блоке подстановки (см. Приложение В). Для каждого 4-битного блока вычислим его адрес в таблице подстановки. Номер блока соответствует номеру столбца, десятичное значение блока соответствует номеру строки в таблице. Таким образом, 5-тый блок (1011) заменяется заполнением 11-ой строки и пятого столбца в таблице подстановки (1110).

номера блоков

8	7	6	5	4	3	2	1
1000	1110	1000	1011	1110	1001	1001	0000

соответствующие номера строк в таблице подстановки

8 14 8 11 14 9 9 0

заполнение

9 2 3 14 5 15 3 4

результат

1001 0010 0011 1110 0101 1111 0011 0100

3). Циклический сдвиг результата п.2 на 11 бит влево

1111 0010 1111 1001 1010 0100 1001 0001

Таким образом, нашли значение функции f (R0,X0):

1111 0010 1111 1001 1010 0100 1001 0001

II. Вычисляем R1= f(R0,X0) ⊕L0.

Результат преобразования функции f(R0,X0) складываем с L0 по mod2:

L0: 1100 1010 1100 1110 1100 0111 1100 1000

f(R0,X0): 1111 0010 1111 1001 1010 0100 1001 0001

R1: 0011 1000 0011 0111 0110 0011 0101 1001

Задание 8. Алгоритм шифрования RSA

Сгенерируйте открытый и закрытый ключи в алгоритме шифрования RSA, выбрав простые числа p и q из первой сотни. Зашифруйте сообщение, состоящее из ваших инициалов: ФИО. Составьте блок-схему и программу алгоритма шифрования RSA. Проверьте результаты программой шифрования.

Пример выполнения

I. Генерация ключей.

Выберем два простых числа $p = 13$ и $q = 19$ (см. Приложение Г). Тогда модуль $n = pq$=13*19 = 247 и функция Эйлера $\varphi(n) = (p-1)(q-1)$ = 12*18 = 216.

Закрытый ключ d выбираем из условий $d < \varphi(n)$ и d взаимно просто с $\varphi(n)$, т.е. d и $\varphi(n)$ не имеют общих делителей. Пусть d = 25.

Открытый ключ e выбираем из условий $e<\varphi(n)$ и $de=1(mod\ \varphi(n))$: e<216,

$25e=1(\text{mod } 216)$. Последнее условие означает, что число $25e$-1 должно делиться на 216 без остатка.

Таким образом, для определения e нужно подобрать такое число k, что

$25e-1 = 216\ k$.

При k=14 получаем $25e$=3024+1 или e=121.

В нашем примере (121, 247) – открытый ключ, (25, 247) – секретный ключ.

II. Шифрование.

Представим шифруемое сообщение «КГЛ» как последовательность целых чисел. Пусть буква «К» соответствует числу 12, буква «Г» - числу 4 и буква «Л» - числу 13.

Зашифруем сообщение, используя открытый ключ (121, 247):

$C_1 = (12^{121}) \bmod 247 = 12$

$C_2 = (4^{121}) \bmod 247 = 199$

$C_3 = (13^{121}) \bmod 247 = 91$

Таким образом, исходному сообщению (12, 4, 13) соответствует криптограмма (12, 199, 91).

III. Расшифрование

Расшифруем сообщение (12, 199, 91), пользуясь секретным ключом (25,247):

$M_1 = (12^{25}) \bmod 247 = 12$

$M_2 = (199^{25}) \bmod 247 = 4$

$M_3 = (91^{25}) \bmod 247 = 13$

В результате расшифрования было получено исходное сообщение (12,4,13), т.е. "КГЛ".

Задание 9. Функция хеширования

Найти хеш–образ своей Фамилии, используя хеш–функцию $H_i = (H_{i-1} + M_i)^2 \bmod n$, где n = pq, p, q взять из Задания 7.

Пример выполнения

Хешируемое сообщение «КОЗИНА». Возьмем два простых числа p=13, q=19 (см. Приложение Е). Определим n=pq=13*19=247. Вектор инициализации H_0 выберем равным 8 (выбираем случайным образом). Слово «КОЗИНА» можно представить последовательностью чисел (12, 16, 9, 10, 15, 1) по номерам букв в алфавите. Таким образом,

$n=247, H_0=8, M_1=12, M_2=16, M_3=9, M_4=10, M_5=15, M_6=1.$

Используя формулу $H_i = (H_{i-1} + M_i)^2 \bmod n$, получим хеш-образ сообщения «КОЗИНА»:

$H_1=(H_0+M_1)^2 \bmod n = (8 + 12)^2 \bmod 247 = 400 \bmod 247=153$

$H_2=(H_1+M_2)^2 \bmod n = (153 + 16)^2 \bmod 247 = 28561 \bmod 247= 156$

$H_3=(H_2+M_3)^2 \bmod n = (156 + 9)^2 \bmod 247 = 27225 \bmod 247= 55$

$H_4=(H_3+M_4)^2 \bmod n = (55 + 10)^2 \bmod 247 = 4225 \bmod 247= 26$

$H_5=(H_4+M_5)^2 \bmod n = (26 + 15)^2 \bmod 247 = 1681 \bmod 247= 199$

$H_6=(H_5+M_6)^2 \bmod n = (199 + 1)^2 \bmod 247 = 40000 \bmod 247= 233$

В итоге получаем хеш-образ сообщения «КОЗИНА», равный 233.

Задание 10. Электронная цифровая подпись (ЭЦП)

Используя хеш-образ своей Фамилии, вычислите электронную цифровую подпись по схеме RSA.

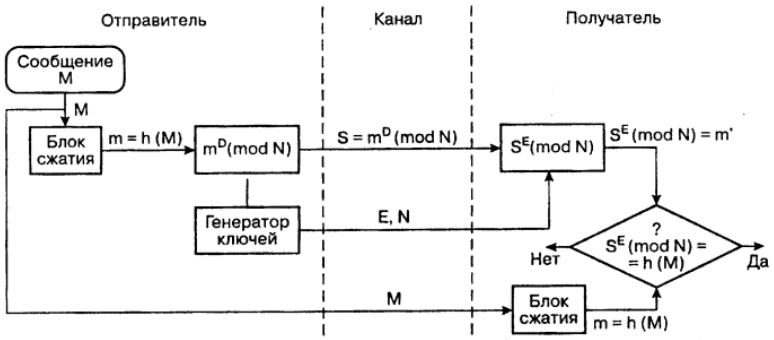

Рис. 1. Схема электронной цифровой подписи RSA

Пример выполнения

Пусть хеш-образ Фамилии равен 233, а закрытый ключ алгоритма RSA равен (25, 247). Тогда электронная цифровая подпись сообщения, состоящего из Фамилии, вычисляется по правилу (см. Приложение Ж)

$$s = 233^{25} \bmod 247 = 168.$$

Для проверки ЭЦП, используя открытый ключ (121, 247), найдем

$$H = 168^{121} \bmod 247 = 233.$$

Поскольку хеш-образ сообщения совпадает с найденным значением H, то подпись признается подлинной.

Приложение А. Таблица Виженера

	А	Б	В	Г	Д	Е	Ё	Ж	З	И	Й	К	Л	М	Н	О	П	Р	С	Т	У	Ф	Х	Ц	Ч	Ш	Щ	Ъ	Ы	Ь	Э	Ю	Я
А	А	Б	В	Г	Д	Е	Ё	Ж	З	И	Й	К	Л	М	Н	О	П	Р	С	Т	У	Ф	Х	Ц	Ч	Ш	Щ	Ъ	Ы	Ь	Э	Ю	Я
Б	Я	А	Б	В	Г	Д	Е	Ё	Ж	З	И	Й	К	Л	М	Н	О	П	Р	С	Т	У	Ф	Х	Ц	Ч	Ш	Щ	Ъ	Ы	Ь	Э	Ю
В	Ю	Я	А	Б	В	Г	Д	Е	Ё	Ж	З	И	Й	К	Л	М	Н	О	П	Р	С	Т	У	Ф	Х	Ц	Ч	Ш	Щ	Ъ	Ы	Ь	Э
Г	Э	Ю	Я	А	Б	В	Г	Д	Е	Ё	Ж	З	И	Й	К	Л	М	Н	О	П	Р	С	Т	У	Ф	Х	Ц	Ч	Ш	Щ	Ъ	Ы	Ь
Д	Ь	Э	Ю	Я	А	Б	В	Г	Д	Е	Ё	Ж	З	И	Й	К	Л	М	Н	О	П	Р	С	Т	У	Ф	Х	Ц	Ч	Ш	Щ	Ъ	Ы
Е	Ы	Ь	Э	Ю	Я	А	Б	В	Г	Д	Е	Ё	Ж	З	И	Й	К	Л	М	Н	О	П	Р	С	Т	У	Ф	Х	Ц	Ч	Ш	Щ	Ъ
Ё	Ъ	Ы	Ь	Э	Ю	Я	А	Б	В	Г	Д	Е	Ё	Ж	З	И	Й	К	Л	М	Н	О	П	Р	С	Т	У	Ф	Х	Ц	Ч	Ш	Щ
Ж	Щ	Ъ	Ы	Ь	Э	Ю	Я	А	Б	В	Г	Д	Е	Ё	Ж	З	И	Й	К	Л	М	Н	О	П	Р	С	Т	У	Ф	Х	Ц	Ч	Ш
З	Ш	Щ	Ъ	Ы	Ь	Э	Ю	Я	А	Б	В	Г	Д	Е	Ё	Ж	З	И	Й	К	Л	М	Н	О	П	Р	С	Т	У	Ф	Х	Ц	Ч
И	Ч	Ш	Щ	Ъ	Ы	Ь	Э	Ю	Я	А	Б	В	Г	Д	Е	Ё	Ж	З	И	Й	К	Л	М	Н	О	П	Р	С	Т	У	Ф	Х	Ц
Й	Ц	Ч	Ш	Щ	Ъ	Ы	Ь	Э	Ю	Я	А	Б	В	Г	Д	Е	Ё	Ж	З	И	Й	К	Л	М	Н	О	П	Р	С	Т	У	Ф	Х
К	Х	Ц	Ч	Ш	Щ	Ъ	Ы	Ь	Э	Ю	Я	А	Б	В	Г	Д	Е	Ё	Ж	З	И	Й	К	Л	М	Н	О	П	Р	С	Т	У	Ф
Л	Ф	Х	Ц	Ч	Ш	Щ	Ъ	Ы	Ь	Э	Ю	Я	А	Б	В	Г	Д	Е	Ё	Ж	З	И	Й	К	Л	М	Н	О	П	Р	С	Т	У
М	У	Ф	Х	Ц	Ч	Ш	Щ	Ъ	Ы	Ь	Э	Ю	Я	А	Б	В	Г	Д	Е	Ё	Ж	З	И	Й	К	Л	М	Н	О	П	Р	С	Т
Н	Т	У	Ф	Х	Ц	Ч	Ш	Щ	Ъ	Ы	Ь	Э	Ю	Я	А	Б	В	Г	Д	Е	Ё	Ж	З	И	Й	К	Л	М	Н	О	П	Р	С
О	С	Т	У	Ф	Х	Ц	Ч	Ш	Щ	Ъ	Ы	Ь	Э	Ю	Я	А	Б	В	Г	Д	Е	Ё	Ж	З	И	Й	К	Л	М	Н	О	П	Р
П	Р	С	Т	У	Ф	Х	Ц	Ч	Ш	Щ	Ъ	Ы	Ь	Э	Ю	Я	А	Б	В	Г	Д	Е	Ё	Ж	З	И	Й	К	Л	М	Н	О	П
Р	П	Р	С	Т	У	Ф	Х	Ц	Ч	Ш	Щ	Ъ	Ы	Ь	Э	Ю	Я	А	Б	В	Г	Д	Е	Ё	Ж	З	И	Й	К	Л	М	Н	О

С	О	П	Р	С	Т	У	Ф	Х	Ц	Ч	Ш	Щ	Ъ	Ы	Ь	Э	Ю	Я	А	Б	В	Г	Д	Е	Ё	Ж	З	И	Й	К	Л	М	Н
Т	Н	О	П	Р	С	Т	У	Ф	Х	Ц	Ч	Ш	Щ	Ъ	Ы	Ь	Э	Ю	Я	А	Б	В	Г	Д	Е	Ё	Ж	З	И	Й	К	Л	М
У	М	Н	О	П	Р	С	Т	У	Ф	Х	Ц	Ч	Ш	Щ	Ъ	Ы	Ь	Э	Ю	Я	А	Б	В	Г	Д	Е	Ё	Ж	З	И	Й	К	Л
Ф	Л	М	Н	О	П	Р	С	Т	У	Ф	Х	Ц	Ч	Ш	Щ	Ъ	Ы	Ь	Э	Ю	Я	А	Б	В	Г	Д	Е	Ё	Ж	З	И	Й	К
Х	К	Л	М	Н	О	П	Р	С	Т	У	Ф	Х	Ц	Ч	Ш	Щ	Ъ	Ы	Ь	Э	Ю	Я	А	Б	В	Г	Д	Е	Ё	Ж	З	И	Й
Ц	Й	К	Л	М	Н	О	П	Р	С	Т	У	Ф	Х	Ц	Ч	Ш	Щ	Ъ	Ы	Ь	Э	Ю	Я	А	Б	В	Г	Д	Е	Ё	Ж	З	И
Ч	И	Й	К	Л	М	Н	О	П	Р	С	Т	У	Ф	Х	Ц	Ч	Ш	Щ	Ъ	Ы	Ь	Э	Ю	Я	А	Б	В	Г	Д	Е	Ё	Ж	З
Ш	З	И	Й	К	Л	М	Н	О	П	Р	С	Т	У	Ф	Х	Ц	Ч	Ш	Щ	Ъ	Ы	Ь	Э	Ю	Я	А	Б	В	Г	Д	Е	Ё	Ж
Щ	Ж	З	И	Й	К	Л	М	Н	О	П	Р	С	Т	У	Ф	Х	Ц	Ч	Ш	Щ	Ъ	Ы	Ь	Э	Ю	Я	А	Б	В	Г	Д	Е	Ё
Ъ	Ё	Ж	З	И	Й	К	Л	М	Н	О	П	Р	С	Т	У	Ф	Х	Ц	Ч	Ш	Щ	Ъ	Ы	Ь	Э	Ю	Я	А	Б	В	Г	Д	Е
Ы	Е	Ё	Ж	З	И	Й	К	Л	М	Н	О	П	Р	С	Т	У	Ф	Х	Ц	Ч	Ш	Щ	Ъ	Ы	Ь	Э	Ю	Я	А	Б	В	Г	Д
Ь	Д	Е	Ё	Ж	З	И	Й	К	Л	М	Н	О	П	Р	С	Т	У	Ф	Х	Ц	Ч	Ш	Щ	Ъ	Ы	Ь	Э	Ю	Я	А	Б	В	Г
Э	Г	Д	Е	Ё	Ж	З	И	Й	К	Л	М	Н	О	П	Р	С	Т	У	Ф	Х	Ц	Ч	Ш	Щ	Ъ	Ы	Ь	Э	Ю	Я	А	Б	В
Ю	В	Г	Д	Е	Ё	Ж	З	И	Й	К	Л	М	Н	О	П	Р	С	Т	У	Ф	Х	Ц	Ч	Ш	Щ	Ъ	Ы	Ь	Э	Ю	Я	А	Б
Я	Б	В	Г	Д	Е	Ё	Ж	З	И	Й	К	Л	М	Н	О	П	Р	С	Т	У	Ф	Х	Ц	Ч	Ш	Щ	Ъ	Ы	Ь	Э	Ю	Я	А

Приложение Б. Символы кириллицы (альтернативная кодовая таблица ASCII)

Сим-л	Дес.	Двоич.	Сим-л	Дес.	Двоич.
А	192	11000000	б	225	11100001
Б	193	11000001	в	226	11100010
В	194	11000010	г	227	11100011
Г	195	11000011	д	228	11100100
Д	196	11000100	е	229	11100101
Е	197	11000101	ж	230	11100110
Ж	198	11000110	з	231	11100111
З	199	11000111	и	232	11101000
И	200	11001000	й	277	11101001
Й	201	11001001	к	234	11101010
К	202	11001010	л	235	11101011
Л	203	11001011	м	236	11101100
М	204	11001100	н	237	11101101
Н	205	11001101	о	238	11101110
О	206	11001110	п	239	11101111
П	207	11001111	р	240	11110000
Р	208	11010000	с	241	11110001
С	209	11010001	т	242	11110010
Т	210	11010010	у	243	11110011
У	211	11010011	ф	244	11110100

Ф	212	11010100	х	245	11110101
Х	213	11010101	ц	246	11110110
Ц	214	11010110	ч	247	11110111
Ч	215	11010111	ш	248	11111000
Ш	216	11011000	щ	249	11111001
Щ	217	11011001	ъ	250	11111010
Ъ	218	11011010	ы	251	11111011
Ы	219	11011011	ь	252	11111100
Ь	220	11011100	э	253	11111101
Э	221	11011101	ю	254	11111110
Ю	222	11011110	я	255	11111111
Я	223	11011111	пробел	32	00010000
а	224	11100000			

Приложение В. Блок подстановки в алгоритме шифрования ГОСТ 28147-89

	8	7	6	5	4	3	2	1
0	1	13	4	6	7	5	14	4
1	15	11	11	12	13	8	11	10
2	13	4	10	7	10	1	4	9
3	0	1	0	1	1	13	12	2
4	5	3	7	5	0	10	6	13
5	7	15	2	15	8	3	13	8
6	10	5	1	13	9	4	15	0
7	4	9	13	8	15	2	10	14
8	9	0	3	4	14	14	2	6
9	2	10	6	10	4	15	3	11
10	3	14	8	9	6	12	8	1
11	14	7	5	14	12	7	1	12
12	6	6	9	0	11	6	0	7
13	11	8	12	3	2	0	7	15
14	8	2	15	11	5	9	5	5
15	12	12	14	2	3	11	9	3

Пример. Пусть 32-битная последовательность имеет вид

1001	1011	1100	0101	1110	0100	0000	1001

Разобьем входную последовательность на 8 блоков по 4 бита. Шестой блок 1100 пропускаем через 6-ой узел подстановки по следующему правилу: преобразуем двоичное число 1100 к десятичному виду – 12. Заполнение 12-ой строки для 6-ого узла подстановки равно 9, что в двоичном виде есть 1001. Таким образом, 4-битный блок 1100 заменяется на 1001. Остальные блоки заменяются аналогично.

8	7	6	5	4	3	2	1	номер узла
1001	1011	1100	0101	1110	0100	0000	1001	вход
9	11	12	5	14	4	0	9	адрес
2	7	9	15	5	10	14	11	заполнение
0010	0111	1001	1111	0101	1010	1110	1011	результат

Выходная последовательность имеет вид

0010	0111	1001	1111	0101	1010	1110	1011

Приложение Г. Таблица простых чисел

1	2	3	5	7
11	13	17	19	23
29	31	37	41	43
47	53	59	61	67
71	73	79	83	89
97	101	103	107	109
113	127	131	137	139
149	151	157	163	167
173	179	181	191	193
197	199	211	223	227
229	233	239	241	251
257	263	269	271	277
281	283	293	307	311
313	317	331	337	347
349	353	359	367	373
379	383	389	397	401
409	419	421	431	433
439	443	449	457	461
463	467	479	487	491
499	503	509	521	523
541	547	557	563	569
571	577	587	593	599

Описание методики оценивания:

Контрольная работа проводится с целью обеспечения своевременной обратной связи, для коррекции обучения, активизации самостоятельной работы студентов. Критериями оптимального усвоения знаний при проведении контрольной работы являются объем, системность, осмысленность, прочность и действенность знаний обучающихся.

Результаты контрольной работы оцениваются в соответствии с рейтинг-планом дисциплины.

Критерии оценки (в баллах)

11-15 – баллов выставляется студенту, если он правильно выполняет задание, демонстрирует его решение и отвечает на дополнительные вопросы;

6-10 – баллов выставляется студенту, если он правильно выполняет задание и отвечает на дополнительные вопросы;

1-5 – баллов выставляется студенту, если он выполняет задание при помощи наводящих вопросов и/или не отвечает на дополнительные вопросы;

0 – баллов выставляется студенту, если он не может выполнить задание и ответить на дополнительные вопросы.

Перечень вопросов к зачету

1. История вопроса становления теории информационной безопасности
2. Предметная область теории информационной безопасности
3. Систематизация понятий в области защиты информации
4. Основные термины и определения правовых понятий в области информационных отношений и защиты информации
5. Понятия предметной области «Защита информации»
6. Основные принципы построения систем защиты
7. Концепция комплексной защиты информации
8. Задачи защиты информации
9. Средства реализации комплексной защиты
10. Понятие об информации как объекте защиты
11. Уровни представления информации
12. Основные свойства защищаемой информации
13. Виды и формы представления информации. Информационные ресурсы
14. Структура и шкала ценности информации. Классификация информационных ресурсов
15. Правовой режим информационных ресурсов
16. Информационная безопасность и ее место в системе национальной безопасности РФ
17. Органы обеспечения информационной безопасности и защиты информации, их функции и задачи, нормативная деятельность
18. Анализ уязвимостей системы с точки зрения угроз информационной безопасности
19. Классификация угроз информационной безопасности.
20. Основные направления и методы реализации угроз
21. Неформальная модель нарушителя
22. Оценка уязвимости системы
23. Определение и основные способы несанкционированного доступа
24. Методы защиты от несанкционированного доступа
25. Организационные методы защиты от несанкционированного доступа
26. Инженерно-технические методы защиты от несанкционированного доступа.
27. Построение систем защиты от угрозы утечки по техническим каналам
28. Идентификация и аутентификация.
29. Основные направления и цели использования криптографических методов

30. Защита от угрозы нарушения конфиденциальности на уровне содержания информации
31. Защита целостности информации при хранении
32. Защита целостности информации при обработке
33. Защита целостности информации при транспортировке
34. Защита от угрозы нарушения целостности информации на уровне содержания
35. Построение систем защиты от угрозы отказа доступа к информации
36. Защита семантического анализа и актуальности информации
37. Политика безопасности
38. Субъектно-объектные модели разграничения доступа
39. Аксиомы политики безопасности
40. Политика и модели дискреционного доступа
41. Парольные системы разграничения доступа
42. Политика и модели мандатного доступа
43. Теоретико-информационные модели
44. Политика и модели тематического разграничения доступа
45. Ролевая модель безопасности
46. Роль стандартов информационной безопасности
47. Критерии безопасности компьютерных систем министерства обороны США (Оранжевая книга),TCSEC
48. Европейские критерии безопасности информационных технологий (ITSEC)
49. Федеральные критерии безопасности информационных технологий США
50. Единые критерии безопасности информационных технологий
51. Группа международных стандартов 270000
52. Определение и основные виды информационных войн
53. Информационно-техническая война
54. Информационно-психологическая война

3. Методические материалы, определяющие процедуры оценивания результатов обучения по дисциплине (модулю), описание шкал оценивания

Рейтинг-план дисциплины

№ п/п	Виды учебной деятельности студентов	Балл за конкретное задание	Число заданий за семестр	Баллы	
				Минимальный	Максимальный
Модуль 1				**0**	**50**
Текущий контроль, в том числе					**25**
1.	Аудиторная работа на практических занятиях (устный опрос)	1	5	0	5
2.	Выполнение и отчет лабораторной работы	5	4	0	20
Рубежный контроль, в том числе				**0**	**25**
1.	Контрольная работа	3	5	0	15
2.	Тестирование	10	1		10
			Итого	**0**	**50**

Модуль 2				**0**	**50**
Текущий контроль, в том числе					**25**
1.	Аудиторная работа на практических занятиях (устный опрос)	1	5	0	5
2.	Выполнение и отчет лабораторной работы	5	4	0	20
Рубежный контроль, в том числе				**0**	**25**
1.	Контрольная работа	3	5	0	15
2.	Тестирование	10	1		10
			Итого	**0**	**50**
Итоговый контроль					
Зачет		0	0	**0**	**0**
Поощрительные баллы					**10**
1.	Выступление на семинаре кафедры	5	1		5
2.	Участие в конференции	5	1		5
			Итого	**0**	**110**
Посещаемость (баллы вычитаются из общей суммы набранных баллов)					
1.	Посещение лекционных занятий			0	-6
2.	Посещение практических занятий			0	-10

Код и наименование индикатора достижения компетенции	**Результаты обучения по дисциплине**	**Оценочные средства**
ОПК-4.1. *знать и понимать принципы работы современных информационных технологий и программных средств, в том числе отечественного производства при решении задач профессиональной деятельности*	*знать: способы получения на основе информационных технологий новых знаний для решения профессиональных задач с учетом требований информационной безопасности и причин нарушения безопасности компьютерных систем.*	*Устный опрос*
ОПК-4.2. *уметь выбирать современные информационные технологии и программные средства, в том числе отечественного производства при решении задач профессиональной деятельности*	*уметь: применять информационные технологии и программные средства, в том числе отечественного производства, для анализа и оценивания эффективности средств защиты информации;* *ориентироваться в современных и перспективных методах защиты информации.*	*Тестовые задания*
ОПК-4.3. *иметь практический опыт применения современных информационных технологий и программных средств, в том числе отечественного производства, при решении*	*владеть: навыками применения методов защиты информации в компьютерных системах; иметь практический опыт применения современных информационных технологий и программных средств, в том числе отечественного*	*Лабораторная работа*

задач профессиональной деятельности	*производства, при решении задач профессиональной деятельности*	
УК-2.1. *Реализует нормы права при решении задач в рамках поставленной цели*	*знать: правовые нормы и методологические основы принятия управленческого решения*	*Устный опрос*
УК-2.2. *Умеет проводить анализ поставленной цели и формулировать задачи, которые необходимо решить для ее достижения; анализировать альтернативные варианты для достижения намеченных результатов; использовать нормативно-правовую документацию в сфере профессиональной деятельности*	*уметь: анализировать альтернативные варианты решений для достижения намеченных результатов; разрабатывать план, определять целевые этапы и основные направления работ.*	*Тестовые задания*
УК-2.3. *Владеет методиками разработки цели и задач проекта; методами оценки потребности в ресурсах, продолжительности и стоимости проекта; навыками работы с нормативно правовой документацией*	*владеть: методиками разработки цели и задач проекта; методами оценки продолжительности и стоимости проекта, а также потребности в ресурсах.*	*Контрольная работа*

Результаты обучения по дисциплине (модулю) у обучающихся оцениваются по итогам текущего контроля количественной оценкой, выраженной в рейтинговых баллах. Оценке подлежит каждое контрольное мероприятие.

При оценивании сформированности компетенций применяется четырехуровневая шкала «неудовлетворительно», «удовлетворительно», «хорошо», «отлично».

Максимальный балл по каждому виду оценочного средства определяется в рейтинг-плане и выражает полное (100%) освоение компетенции.

Уровень сформированности компетенции «хорошо» устанавливается в случае, когда объем выполненных заданий соответствующего оценочного средства составляет 80-100%; «удовлетворительно» – выполнено 40-80%; «неудовлетворительно» – выполнено 0-40%

Рейтинговый балл за выполнение части или полного объема заданий соответствующего оценочного средства выставляется по формуле:

Рейтинговый балл = k × Максимальный балл,

где k = 0,2 при уровне освоения «неудовлетворительно», k = 0,4 при уровне освоения «удовлетворительно», k = 0,8 при уровне освоения «хорошо» и k = 1 при уровне освоения «отлично».

Оценка на этапе промежуточной аттестации выставляется согласно Положению о модульно-рейтинговой системе обучения и оценки успеваемости студентов УУНиТ:

На зачете выставляется оценка:

• зачтено - при накоплении от 60 до 110 рейтинговых баллов (включая 10 поощрительных

баллов),
• не зачтено - при накоплении от 0 до 59 рейтинговых баллов.

При получении на экзамене оценок «отлично», «хорошо», «удовлетворительно», на зачёте оценки «зачтено» считается, что результаты обучения по дисциплине (модулю) достигнуты и компетенции на этапе изучения дисциплины (модуля) сформированы.