МИНИСТЕРСТВО НАУКИ И ВЫСШЕГО ОБРАЗОВАНИЯ РОССИЙСКОЙ ФЕДЕРАЦИИ
Федеральное государственное автономное образовательное учреждение высшего образования
«Казанский (Приволжский) федеральный университет»
Елабужский институт (филиал) КФУ

УТВЕРЖДАЮ
Директор
Елабужского института КФУ
_____ Е.Е. Мерзон
«22» 05 2024 г.
МП

Программа дисциплины (модуля)
Информационная безопасность

Направление подготовки/специальность: 23.03.01 Технология транспортных процессов
Направленность (профиль) подготовки: Проектирование и управление интеллектуальными транспортными системами
Квалификация выпускника: бакалавр
Форма обучения: заочная
Язык обучения: русский
Год начала обучения по образовательной программе: 2024

Содержание

Программу дисциплины разработал(а)(и) старший преподаватель, б/с Галимуллина Э.З. (Кафедра математики и прикладной информатики).

1. Перечень планируемых результатов обучения по дисциплине (модулю), соотнесенных с планируемыми результатами освоения ОПОП ВО

Обучающийся, освоивший дисциплину (модуль), должен обладать следующими компетенциями:

Шифр компетенции	Расшифровка приобретаемой компетенции
ПК-4	Способен разрабатывать алгоритмы и программы, пригодные для практического применения
ПК-4.1.	Знать технологии разработки алгоритмов и программ, пригодных для практического применения
ПК-4.2.	Уметь разрабатывать алгоритмы и программы, пригодные для практического применения
ПК-4.3.	Владеть способностью разрабатывать алгоритмы и программы, пригодные для практического применения

Обучающийся, освоивший дисциплину (модуль):

Должен знать:
- базовые технологии разработки типовых алгоритмов и программ, пригодных для решения практических задач по информационной безопасности

Должен уметь:
- разрабатывать под руководством наставника типовые алгоритмы и программы, пригодные для решения задач информационной безопасности

Должен владеть:
- способностью разрабатывать под руководством наставника типовые алгоритмы и программы, пригодные для решения практических задач области защиты информации.

2. Место дисциплины (модуля) в структуре ОПОП ВО

Данная дисциплина (модуль) включена в раздел "Б1.В.04.06 Дисциплины (модули)" основной профессиональной образовательной программы 23.03.01 Технология транспортных процессов и относится к части, формируемой участниками образовательных отношений.
Осваивается на 5 курсе в 10 семестре.

3. Объем дисциплины (модуля) в зачетных единицах с указанием количества часов, выделенных на контактную работу обучающихся с преподавателем (по видам учебных занятий) и на самостоятельную работу обучающихся

Общая трудоемкость дисциплины составляет 2 зачетных(ые) единиц(ы) на 72 часа(ов).
Контактная работа - 10 часа(ов), в том числе лекции - 4 часа(ов), практические занятия - 0 часа(ов), лабораторные работы - 6 часа(ов), контроль самостоятельной работы - 0 часа(ов).
Самостоятельная работа - 58 часа(ов).
Контроль (зачёт / экзамен) - 4 часа(ов).
Форма промежуточного контроля дисциплины: зачет в 10 семестре.

4. Содержание дисциплины (модуля), структурированное по темам (разделам) с указанием отведенного на них количества академических часов и видов учебных занятий

4.1 Структура и тематический план контактной и самостоятельной работы по дисциплине (модулю)

N	Разделы дисциплины / модуля	Семестр	Виды и часы контактной работы, их трудоемкость (в часах)			Самостоятельная работа
			Лекции	Практические занятия	Лабораторные работы	
1.	Тема 1. Основные понятия и анализ угроз информационной безопасности.	10	0	0	0	10
2.	Тема 2. Политики безопасности. Модели политик безопасности	10	1	0	0	10
3.	Тема 3. Стандарты информационной безопасности	10	1	0	2	10
4.	Тема 4. Криптографическая защита информации.	10	1	0	2	10
5.	Тема 5. Технологии аутентификации.	10	1	0	2	18
	Итого		4	0	6	58

4.2 Содержание дисциплины (модуля)

Тема 1. Основные понятия и анализ угроз информационной безопасности.

Основные понятия и анализ угроз информационной безопасности. Основные понятия информационной безопасности. Общие понятия информационной безопасности. Анализ угроз информационной безопасности. Классификация угроз информационным системам. Основные методы обеспечения информационной безопасности информационных систем.

Тема 2. Политики безопасности. Модели политик безопасности

Политика безопасности. Общие принципы моделей политик безопасности. Классификация существующих моделей политики информационной безопасности. Свободные и мандатные модели политик безопасности. Модель Белла - Ла-Падулы. Модель Биба. Модель контроля целостности Кларка-Вилсона. Политика избирательного разграничения доступа. Анализ моделей политик безопасности.

Тема 3. Стандарты информационной безопасности

Стандарты информационной безопасности. Роль стандартов информационной безопасности. Международные стандарты информационной безопасности. Отечественные стандарты безопасности информационных технологий. Государственные (национальные) стандарты РФ. Руководящие документы. Нормативные документы информационной безопасности.

Тема 4. Криптографическая защита информации.

Криптографическая защита информации. Основные понятия криптографической защиты информации. Симметричные криптосистемы шифрования. Асимметричные криптосистемы шифрования. Функция хэширования. Электронная цифровая подпись. Методы криптографической защиты информации. Простейшие алгоритмы шифрования (Система шифрования Цезаря, Простая моноалфавитная замена, G-контурная многоалфавитная замена, Простая перестановка, Перестановки Гамильтона). Элементы криптоанализа. Оценка частотности символов в тексте.

Тема 5. Технологии аутентификации.

Технологии аутентификации. Аутентификация, авторизация и администрирование действий пользователей. Методы аутентификации, использующие пароли и PIN-коды. Биометрическая аутентификация пользователя. Аппаратно-программные системы идентификации и аутентификации. Подсистемы парольной аутентификации пользователей. Генераторы паролей. Оценка степени стойкости парольной защиты. Биометрическая аутентификация пользователя по клавиатурному почерку. Анализ динамики нажатия клавиш.

5. Перечень учебно-методического обеспечения для самостоятельной работы обучающихся по дисциплине (модулю)

Самостоятельная работа обучающихся выполняется по заданию и при методическом руководстве преподавателя, но без его непосредственного участия. Самостоятельная работа подразделяется на самостоятельную работу на аудиторных занятиях и на внеаудиторную самостоятельную работу. Самостоятельная работа обучающихся включает как полностью самостоятельное освоение отдельных тем (разделов) дисциплины, так и проработку тем (разделов), осваиваемых во время аудиторной работы. Во время самостоятельной работы обучающиеся читают и конспектируют учебную, научную и справочную литературу, выполняют задания, направленные на закрепление знаний и отработку умений и навыков, готовятся к текущему и промежуточному контролю по дисциплине.

Организация самостоятельной работы обучающихся регламентируется нормативными документами, учебно-методической литературой и электронными образовательными ресурсами, включая:

Порядок организации и осуществления образовательной деятельности по образовательным программам высшего образования - программам бакалавриата, программам специалитета, программам магистратуры (утвержден приказом Министерства образования и науки Российской Федерации от 5 апреля 2017 года №301)

Письмо Министерства образования Российской Федерации №14-55-996ин/15 от 27 ноября 2002 г. "Об активизации самостоятельной работы студентов высших учебных заведений"

Устав федерального государственного автономного образовательного учреждения "Казанский (Приволжский) федеральный университет"

Правила внутреннего распорядка федерального государственного автономного образовательного учреждения высшего профессионального образования "Казанский (Приволжский) федеральный университет"

Локальные нормативные акты Казанского (Приволжского) федерального университета

6. Фонд оценочных средств по дисциплине (модулю)

Фонд оценочных средств по дисциплине (модулю) включает оценочные материалы, направленные на проверку освоения компетенций, в том числе знаний, умений и навыков. Фонд оценочных средств включает оценочные средства текущего контроля и оценочные средства промежуточной аттестации.

В фонде оценочных средств содержится следующая информация:

- соответствие компетенций планируемым результатам обучения по дисциплине (модулю);
- критерии оценивания сформированности компетенций;
- механизм формирования оценки по дисциплине (модулю);
- описание порядка применения и процедуры оценивания для каждого оценочного средства;
- критерии оценивания для каждого оценочного средства;
- содержание оценочных средств, включая требования, предъявляемые к действиям обучающихся, демонстрируемым результатам, задания различных типов.

Фонд оценочных средств по дисциплине находится в Приложении 1 к программе дисциплины (модулю).

7. Перечень литературы, необходимой для освоения дисциплины (модуля)

Освоение дисциплины (модуля) предполагает изучение учебной литературы. Литература может быть доступна обучающимся в одном из двух вариантов (либо в обоих из них):

- в электронном виде - через электронные библиотечные системы на основании заключенных КФУ договоров с правообладателями;
- в печатном виде - в Научной библиотеке Елабужского института КФУ. Обучающиеся получают учебную литературу на абонементе по читательским билетам в соответствии с правилами пользования Научной библиотекой.

Электронные издания доступны дистанционно из любой точки при введении обучающимся своего логина и пароля от личного кабинета в системе "Электронный университет". При использовании печатных изданий библиотечный фонд должен быть укомплектован ими из расчета не менее 0,25 экземпляра на каждого обучающегося из числа лиц, одновременно осваивающих данную дисциплину

Перечень литературы, необходимой для освоения дисциплины (модуля), находится в Приложении 2 к рабочей программе дисциплины. Он подлежит обновлению при изменении условий договоров КФУ с правообладателями электронных изданий и при изменении комплектования фондов Научной библиотеки Елабужского института КФУ.

8. Перечень ресурсов информационно-телекоммуникационной сети "Интернет", необходимых для освоения дисциплины (модуля)

«Антивирусная защита компьютерных систем» НОЧУ ВПО "Национальный открытый университет "ИНТУИТ" - http://www.intuit.ru/studies/courses/2259/155/info

«Основы информационной безопасности» В.Галатенко НОЧУ ВПО "Национальный открытый университет "ИНТУИТ" - http://www.intuit.ru/studies/courses/10/10/info

Каталог информационной системы "Единое окно доступа к образовательным ресурсам" - http://window.edu.ru

9. Методические указания для обучающихся по освоению дисциплины (модуля)

Вид работ	Методические рекомендации
лекции	Лекционные занятия проводятся с использованием интерактивных технологий и предполагают активное участие студентов. Для подготовки к занятиям рекомендуется выделять в материале проблемные вопросы, затрагиваемые преподавателем в лекции, и группировать информацию вокруг них. Желательно выделять в используемой литературе постановки вопросов, на которые разными авторам могут быть даны различные ответы. На основании постановки таких вопросов следует собирать аргументы в пользу различных вариантов решения поставленных проблем.
лабораторные работы	Лабораторные занятия - это одна из разновидностей практического занятия, являющаяся эффективной формой учебных занятий в организации высшего образования. Лабораторные занятия имеют выраженную специфику в зависимости от учебной дисциплины, углубляют и закрепляют теоретические знания. На этих занятиях студенты осваивают конкретные методы изучения дисциплины, обучаются экспериментальным способам анализа, умению работать с приборами и современным оборудованием. Лабораторные занятия дают наглядное представление об изучаемых явлениях и процессах, студенты осваивают постановку и ведение эксперимента, учатся умению наблюдать, оценивать полученные результаты, делать выводы и обобщения. Отчёт по итогам выполненных лабораторных работ выполняется на листах белой бумаги формата А4 в печатном или рукописном виде. При оформлении отчёта используется сквозная нумерация страниц, считая титульный лист первой страницей. Номер страницы на титульном листе не ставится. Номера страницы ставятся по центру вверху. При оформлении отчёта в печатном виде желательно соблюдать следующие требования. Для заголовков: полужирный шрифт, 14 пт, центрированный. Для основного текста: нежирный шрифт, 14 пт, выравнивание по ширине. Во всех случаях тип шрифта - Times New Roman, отступ абзаца 1.25 см, полуторный междустрочный интервал. Поля: левое - 3 см, правое - 1 см, верхнее и нижнее - 2 см. Отчет должен содержать следующие элементы: 1) Титульный лист с обязательным указанием варианта; 2) Цель работы; 3) Задание; 4) Основная часть; 5) Вывод.
самостоя-тельная работа	Самостоятельная работа студентов по дидактической сути представляет собой комплекс условий обучения, организуемых преподавателем и направленных на самоподготовку учащихся. Учебная деятельность протекает без непосредственного участия преподавателя и заключается в проработке лекционного материала, подготовке к лабораторным занятиям; изучении учебной литературы из основного и дополнительного списка.
зачет	Зачет нацелен на комплексную проверку освоения дисциплины. Зачет проводится в устной или письменной форме по билетам, в которых содержатся вопросы (задания) по всем темам курса. Обучающемуся даётся время на подготовку. Оценивается владение материалом, его системное освоение, способность применять нужные знания, навыки и умения при анализе проблемных ситуаций и решении практических заданий.

10. Перечень информационных технологий, используемых при осуществлении образовательного процесса по дисциплине (модулю), включая перечень программного обеспечения и информационных справочных систем (при необходимости)

Перечень информационных технологий, используемых при осуществлении образовательного процесса по дисциплине (модулю), включая перечень программного обеспечения и информационных справочных систем, представлен в Приложении 3 к рабочей программе дисциплины (модуля).

11. Описание материально-технической базы, необходимой для осуществления образовательного процесса по дисциплине (модулю)

Учебные аудитории № 60 (423600, Республика Татарстан, г. Елабуга, ул. Казанская, д. 89) для проведения занятий лекционного типа, занятий семинарского типа, групповых и индивидуальных консультаций, текущего контроля и промежуточной аттестации, помещение для самостоятельной работы. Комплект мебели (посадочных мест) 29 шт. Комплект мебели (посадочных мест) для преподавателя 1 шт. Компьютерный класс: Компьютеры intel core i5 15 шт. Мониторы ViewSonic 22d 15 шт. Проектор EPSON EB-535W 1 шт. Интерактивная доска IQBoard DVT TN082 1 шт. Трибуна 1 шт. Кондиционер 1 шт. Настенные полки 6 шт. Шкаф двухстворчатый с полками 1 шт. Веб-камера 1 шт. Выход в Интернет, внутривузовская компьютерная сеть, доступ в электронную информационно-образовательную среду. Набор учебно-наглядных пособий: комплект презентаций в электронном формате по преподаваемой

дисциплине 3-5 шт.

12. Средства адаптации преподавания дисциплины к потребностям обучающихся инвалидов и лиц с ограниченными возможностями здоровья

При необходимости в образовательном процессе применяются следующие методы и технологии, облегчающие восприятие информации обучающимися инвалидами и лицами с ограниченными возможностями здоровья:

- создание текстовой версии любого нетекстового контента для его возможного преобразования в альтернативные формы, удобные для различных пользователей;
- создание контента, который можно представить в различных видах без потери данных или структуры, предусмотреть возможность масштабирования текста и изображений без потери качества, предусмотреть доступность управления контентом с клавиатуры;
- создание возможностей для обучающихся воспринимать одну и ту же информацию из разных источников - например, так, чтобы лица с нарушениями слуха получали информацию визуально, с нарушениями зрения - аудиально;
- применение программных средств, обеспечивающих возможность освоения навыков и умений, формируемых дисциплиной, за счёт альтернативных способов, в том числе виртуальных лабораторий и симуляционных технологий;
- применение дистанционных образовательных технологий для передачи информации, организации различных форм интерактивной контактной работы обучающегося с преподавателем, в том числе вебинаров, которые могут быть использованы для проведения виртуальных лекций с возможностью взаимодействия всех участников дистанционного обучения, проведения семинаров, выступления с докладами и защиты выполненных работ, проведения тренингов, организации коллективной работы;
- применение дистанционных образовательных технологий для организации форм текущего и промежуточного контроля;
- увеличение продолжительности сдачи обучающимся инвалидом или лицом с ограниченными возможностями здоровья форм промежуточной аттестации по отношению к установленной продолжительности их сдачи:
- продолжительности сдачи зачёта или экзамена, проводимого в письменной форме, - не более чем на 90 минут;
- продолжительности подготовки обучающегося к ответу на зачёте или экзамене, проводимом в устной форме, - не более чем на 20 минут;
- продолжительности выступления обучающегося при защите курсовой работы - не более чем на 15 минут.

Программа составлена в соответствии с требованиями ФГОС ВО и учебным планом по направлению 23.03.01 "Технология транспортных процессов" и профилю подготовки " Проектирование и управление интеллектуальными транспортными системами".

Приложение №1
к рабочей программе дисциплины (модуля)
Б1.В.04.06 Информационная безопасность

МИНИСТЕРСТВО НАУКИ И ВЫСШЕГО ОБРАЗОВАНИЯ РОССИЙСКОЙ ФЕДЕРАЦИИ
Федеральное государственное автономное образовательное учреждение высшего образования
"Казанский (Приволжский) федеральный университет"
Елабужский институт (филиал)

Фонд оценочных средств по дисциплине (модулю)
Б1.В.04.06 Информационная безопасность

Направление подготовки: 23.03.01 Технология транспортных процессов
Профиль подготовки: Проектирование и управление интеллектуальными транспортными системами
Квалификация выпускника: бакалавр
Форма обучения: очное
Язык обучения: русский
Год начала обучения по образовательной программе: 2024

СОДЕРЖАНИЕ

1. Соответствие компетенций планируемым результатам обучения по дисциплине (модулю)

Код и наименование компетенции	**Индикаторы достижения компетенций для данной дисциплины**	**Оценочные средства текущего контроля и промежуточной аттестации**
ПК-4. Способен разрабатывать алгоритмы и программы, пригодные для практического применения	Знает базовые технологии разработки типовых алгоритмов и программ, пригодных для решения практических задач по информационной безопасности Умеет разрабатывать под руководством наставника типовые алгоритмы и программы, пригодные для решения задач информационной безопасности Владеет способностью разрабатывать под руководством наставника типовые алгоритмы и программы, пригодные для решения практических задач области защиты информации	**Текущий контроль:** *Устный опрос* по темам: Тема 1. Основные понятия и анализ угроз информационной безопасности. Тема 2. Политики безопасности. Модели политик безопасности Тема 3. Стандарты информационной безопасности Тема 4. Криптографическая защита информации. Тема 5. Технологии аутентификации. *Реферат* по темам: Тема 1. Основные понятия и анализ угроз информационной безопасности. Тема 2. Политики безопасности. Модели политик безопасности Тема 3. Стандарты информационной безопасности Тема 4. Криптографическая защита информации. Тема 5. Технологии аутентификации. *Лабораторные работы* по темам: Тема 2. Политики безопасности. Модели политик безопасности Тема 4. Криптографическая защита информации. Тема 5. Технологии аутентификации. **Промежуточная аттестация:** *Зачет*

2. Критерии оценивания сформированности компетенций

Компетенция	**Зачтено**			**Не зачтено**
	Высокий уровень (отлично)	**Средний уровень (хорошо)**	**Низкий уровень (удовлетворительно)**	**Ниже порогового уровня (неудовлетворительно)**
ПК-4	Знает базовые технологии разработки типовых алгоритмов и программ, пригодных для решения практических задач по информационной безопасности	Знает основные технологии разработки типовых алгоритмов и программ, пригодных для решения практических задач по информационной безопасности. Допускает незначительные ошибки при ответе на вопрос или решении поставленной задачи.	Знает отдельные технологии разработки типовых алгоритмов и программ, пригодных для решения практических задач по информационной безопасности. Допускает типичные ошибки при ответе на вопрос или решении поставленной задачи.	Не знает базовые технологии разработки типовых алгоритмов и программ, пригодных для решения практических задач по информационной безопасности.
	Умеет разрабатывать под руководством наставника типовые алгоритмы и программы, пригодные для решения	Умеет разрабатывать под руководством наставника типовые алгоритмы и программы, пригодные	Умеет разрабатывать под руководством наставника типовые алгоритмы и программы, пригодные	Не умеет разрабатывать под руководством наставника типовые алгоритмы и программы, пригодные

	задач информационной безопасности	для решения задач информационной безопасности. Допускает незначительные ошибки при ответе на вопрос или решении поставленной задачи.	для решения задач информационной безопасности. Допускает типичные ошибки при ответе на вопрос или решении поставленной задачи.	для решения задач информационной безопасности
	Владеет способностью разрабатывать под руководством наставника типовые алгоритмы и программы, пригодные для решения практических задач области защиты информации	Владеет способностью разрабатывать под руководством наставника типовые алгоритмы и программы, пригодные для решения практических задач области защиты информации. Допускает незначительные ошибки при ответе на вопрос или решении поставленной задачи	Владеет навыками определения основных и специфических задач в рамках поставленной цели, выбора способов их решения, методиками разработки цели и задач проекта; способностью руководить управлением инновационными проектами создания информационных систем на стадиях жизненного цикла. Допускает типичные ошибки при ответе на вопрос или решении поставленной задачи	Не владеет способностью разрабатывать под руководством наставника типовые алгоритмы и программы, пригодные для решения практических задач области защиты информации

3. Распределение оценок за формы текущего контроля и промежуточную аттестацию

10 семестр:
Текущий контроль:
Устный опрос. Тема 1. Основные понятия и анализ угроз информационной безопасности. Тема 2. Политики безопасности. Модели политик безопасности. Тема 3. Стандарты информационной безопасности. Тема 4. Криптографическая защита информации. Тема 5. Технологии аутентификации.
Реферат. Тема 1. Основные понятия и анализ угроз информационной безопасности. Тема 2. Политики безопасности. Модели политик безопасности. Тема 3. Стандарты информационной безопасности. Тема 4. Криптографическая защита информации. Тема 5. Технологии аутентификации.
Лабораторные работы. Тема 2. Политики безопасности. Модели политик безопасности. Тема 4. Криптографическая защита информации. Тема 5. Технологии аутентификации.

Выполнение каждого оценочного средства оценивается по шкале: отлично, хорошо, удовлетворительно, неудовлетворительно.
Общая оценка за текущий контроль представляет собой среднее значение между полученными оценками за все оценочные средства.

Промежуточная аттестация - зачет**.**
Промежуточная аттестация проводится после завершения изучения дисциплины или ее части в форме, определяемой учебным планом образовательной программы с целью оценить работу обучающегося, степень усвоения теоретических знаний, уровень сформированности компетенций.
Преподаватель, принимающий зачет обеспечивает случайное распределение вариантов зачетных заданий между обучающимися с помощью билетов и/или с применением компьютерных технологий; вправе задавать обучающемуся дополнительные вопросы и давать дополнительные задания помимо тех, которые указаны в билете.
Зачет проводится по билетам. В каждом билете два оценочных средства: устный или письменный ответ на вопрос и решение задачи.

Выполнение каждого задания за промежуточную аттестацию оценивается по шкале: отлично, хорошо, удовлетворительно, неудовлетворительно.
Общая оценка за промежуточную аттестацию представляет собой среднее значение между полученными оценками за все оценочные средства промежуточной аттестации.

В случае невозможности установления среднего значения оценки за промежуточную аттестацию (например, «хорошо» или «отлично»), итоговая оценка выставляется преподавателем, исходя из принципа справедливости и беспристрастности на основании общего впечатления о качестве и добросовестности освоения обучающимся дисциплины (модуля).

Соответствие оценок:
Для зачета:

зачтено
не зачтено

4. Оценочные средства, порядок их применения и критерии оценивания

4.1. Устный опрос. Тема 1. Основные понятия и анализ угроз информационной безопасности. Тема 2. Политики безопасности. Модели политик безопасности. Тема 3. Стандарты информационной безопасности. Тема 4. Криптографическая защита информации. Тема 5. Технологии аутентификации.

4.1.1.1. Порядок проведения и процедура оценивания.

Устный опрос проводится на практических занятиях. Обучающиеся выступают с докладами, сообщениями, дополнениями, участвуют в дискуссии, отвечают на вопросы преподавателя. Оценивается уровень домашней подготовки по теме, способность системно и логично излагать материал, анализировать, формулировать собственную позицию, отвечать на дополнительные вопросы.

4.1.1.2 Критерии оценивания

«Оценка «отлично» ставится, если обучающийся:
В ответе качественно раскрыл содержание темы. Ответ хорошо структурирован. Прекрасно освоен понятийный аппарат. Продемонстрирован высокий уровень понимания материала. Превосходное умение формулировать свои мысли, обсуждать дискуссионные положения.
Оценка «хорошо» ставится, если обучающийся:
Основные вопросы темы раскрыл. Структура ответа в целом адекватна теме. Хорошо освоен понятийный аппарат. Продемонстрирован хороший уровень понимания материала. Хорошее умение формулировать свои мысли, обсуждать дискуссионные положения.
Оценка «удовлетворительно» ставится, если обучающийся:
Тему частично раскрыл. Ответ слабо структурирован. Понятийный аппарат освоен частично. Понимание отдельных положений из материала по теме. Удовлетворительное умение формулировать свои мысли, обсуждать дискуссионные положения.
«Оценка «неудовлетворительно» ставится, если обучающийся:
Тему не раскрыл. Понятийный аппарат освоен неудовлетворительно. Понимание материала фрагментарное или отсутствует. Неумение формулировать свои мысли, обсуждать дискуссионные положения.

4.1.1.3. Содержание оценочного средства
Темы 1-5
1. Охарактеризуйте направление "криптография". Что называют криптографическим ключом?
2. Проклассифицируйте традиционные алгоритмы шифрования. Кратко охарактеризуйте эти классы.
3. Охарактеризуйте методы шифрования Цезаря, простую моноалфавитную замену, G-контурную многоалфавитную замену, простую перестановку, перестановки Гамильтона.
4. Что понимается под криптоанализом?
5. Что понимают под криптоанализом?
6. Охарактеризуйте методику криптоанализа, основанную на исследовании частотности закрытого текста.
7. Сформулируйте правило А. Керхоффа.
8. Что понимается под идентификацией и аутентификацией пользователя?
9. Чем определяется стойкость к взлому подсистемы идентификации и аутентификации пользователя?
10. Перечислите основные требования к выбору пароля и к реализации подсистемы парольной аутентификации пользователя.
11. Как количественно оценить стойкость подсистемы парольной аутентификации к взлому?
12. Как изменится стойкость к взлому подсистемы парольной аутентификации при увеличении характеристик P,V,T? При их уменьшении?

4.1.2. Реферат. Тема 1. Основные понятия и анализ угроз информационной безопасности. Тема 2. Политики безопасности. Модели политик безопасности. Тема 3. Стандарты информационной безопасности. Тема 4. Криптографическая защита информации. Тема 5. Технологии аутентификации.

4.1.2.1. Порядок проведения и процедура оценивания.

Обучающиеся самостоятельно пишут работу на заданную тему и сдают преподавателю в письменном виде. В работе производится обзор материала в определённой тематической области либо предлагается собственное решение определённой теоретической или практической проблемы. Оцениваются проработка источников, изложение материала, формулировка выводов, соблюдение требований к структуре и оформлению работы, своевременность выполнения. В случае публичной защиты реферата оцениваются также ораторские способности.

4.1.2.2 Критерии оценивания

«Оценка «отлично» ставится, если обучающийся:
В ответе качественно раскрыл содержание темы. Ответ хорошо структурирован. Прекрасно освоен понятийный аппарат. Продемонстрирован высокий уровень понимания материала. Превосходное умение формулировать свои мысли, обсуждать дискуссионные положения.
«Оценка «хорошо» ставится, если обучающийся:
Основные вопросы темы раскрыл. Структура ответа в целом адекватна теме. Хорошо освоен понятийный аппарат. Продемонстрирован хороший уровень понимания материала. Хорошее умение формулировать свои мысли, обсуждать дискуссионные положения.
«Оценка «удовлетворительно» ставится, если обучающийся:
Тему частично раскрыл. Ответ слабо структурирован. Понятийный аппарат освоен частично. Понимание отдельных положений из материала по теме. Удовлетворительное умение формулировать свои мысли, обсуждать дискуссионные положения.
Оценка «неудовлетворительно» ставится, если обучающийся:
Тему не раскрыл. Понятийный аппарат освоен неудовлетворительно. Понимание материала фрагментарное или отсутствует. Неумение формулировать свои мысли, обсуждать дискуссионные положения.

4.1.2.3. Содержание оценочного средства

Темы 1-5
Примерные темы рефератов:
1. Технические каналы утечки информации.
2. Выявление технических каналов утечки информации.
3. Организация и проведение поисковых мероприятий на объекте с целью обнаружения каналов утечки информации, выявления средств съема информации.
4. Методы и средства защиты информации от утечки по техническим каналам.
5. Информационная безопасность в среде Windows NT.
6. Информационная безопасность на основе Novell NetWare
7. Информационная безопасность на основе Unix.
8. Вопросы безопасности электронной торговли.
9. Защита Internet-торговли: инфраструктура и стандарты.
10. Криптография для электронной коммерции.
11. Нормативно-правовые аспекты электронного бизнеса.
12. Безопасность при работе в Интернет.
13. Стеганография - искусство сокрытия самого факта передачи информации
14. Интеллектуальная собственность в области программных продуктов.
15. Защита баз данных.
16. Защита от несанкционированного доступа.
17. Вирусы и вредоносные программы.
18. Комплексное обеспечение информационной безопасности в коммерческих структурах.
19. Исследование места и роли проблем информационной безопасности в становлении современного информационного общества.
20. Исследование проблем обеспечения баланса интересов личности, общества и государства в информационной сфере.
21. Исследование роли и места информационной безопасности в обеспечении военной, экономической, экологической, иных видов национальной безопасности.
22. Национальные интересы России и информационное противостояние в современном мире.
23. Ценностная ориентация личности, ее информационное обоснование.
24. Информационная безопасность и политическая этика.

25. Информационное пространство и проблема целостности российского государства.
26. Исследование места и роли СМИ в решении задач информационного обеспечения государственной политики Российской Федерации.
27. Правовые механизмы регулирования в сфере производства и эксплуатации криптографических продуктов.
28. Разработка правовых механизмов регулирования электронного документооборота.
29. Проблемы правового обеспечения создания и функционирования системы мониторинга угроз информационных атак на критически важные сегменты информационной инфраструктуры Российской Федерации.
30. Разработка и научное обоснование путей обеспечения информационно-психологической безопасности личности и общества.

4.1.3. Лабораторные работы. Тема 2. Политики безопасности. Модели политик безопасности. Тема 4. Криптографическая защита информации. Тема 5. Технологии аутентификации.

4.1.3.1. Порядок проведения и процедура оценивания.

На лабораторных занятиях студенты решают типовые задачи с использованием информационных технологий. Работа на лабораторных занятиях предполагает повторение теоретического материала, активное участие в совместном решении задач, отчеты по выполненной домашней работе. При подготовке к занятиям следует ориентироваться на конспекты лекций, а также учебники из рекомендованного списка литературы.

4.1.3.2 Критерии оценивания

Оценка «отлично» ставится, если обучающийся:
Правильно выполнил все задания. Продемонстрировал высокий уровень владения материалом. Проявлены превосходные способности применять знания и умения к выполнению конкретных заданий.
Оценка «хорошо» ставится, если обучающийся:
Правильно выполнил большую часть заданий. Присутствуют незначительные ошибки. Продемонстрирован хороший уровень владения материалом. Проявлены средние способности применять знания и умения к выполнению конкретных заданий.
Оценка «удовлетворительно» ставится, если обучающийся:
Задания выполнил более чем наполовину. Присутствуют серьёзные ошибки. Продемонстрирован удовлетворительный уровень владения материалом. Проявлены низкие способности применять знания и умения к выполнению конкретных заданий.
Оценка «неудовлетворительно» ставится, если обучающийся:
Задания выполнил менее чем наполовину. Продемонстрирован неудовлетворительный уровень владения материалом. Проявлены недостаточные способности применять знания и умения к выполнению конкретных заданий.

4.1.3.3. Содержание оценочного средства

Темы 2, 4, 5
Лабораторная работа 1 «Методы криптографической защиты информации. Простейшие алгоритмы шифрования (Система шифрования Цезаря, Простая моноалфавитная замена, G-контурная многоалфавитная замена, Простая перестановка, Перестановки Гамильтона)».
Лабораторная работа 2 «Элементы криптоанализа. Оценка частотности символов в тексте».
Лабораторная работа 3 «Подсистемы парольной аутентификации пользователей. Генераторы паролей. Оценка степени стойкости парольной защиты».

Пример лабораторной работы № 1
«Методы криптографической защиты информации
Простейшие алгоритмы шифрования»

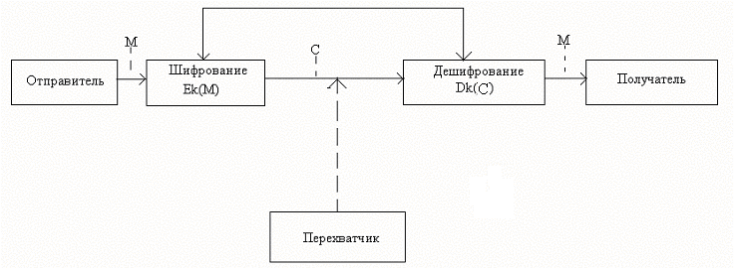
Цель работы – изучение простейших традиционных алгоритмов криптографической защиты информации и особенностей их практической реализации.

Теоретический материал

Криптография

Криптография представляет собой совокупность методов преобразования данных, направленных на то, чтобы сделать эти данные бесполезными для противника. Такие преобразования позволяют решить две главные проблемы защиты данных: проблему обеспечения *конфиденциальности* (путем лишения противника возможности извлечь информацию из канала связи) и проблему *целостности* (путем лишения противника возможности изменить сообщение так, чтобы изменился его смысл, или ввести ложную информацию в канал связи).
Обобщенная схема криптографической системы, обеспечивающей шифрование передаваемой информации, изображена на следующем рисунке:

Ключ К



Отправитель генерирует *открытый текст* исходного сообщения *M*, которое должно быть передано законному получателю по незащищенному каналу. За каналом следит перехватчик с целью перехватить и раскрыть передаваемое сообщение. Для того, чтобы перехватчик не смог узнать содержание сообщения *M*, отправитель шифрует его с помощью обратимого преобразования E_k и получает *шифротекст* $C=E_k(M)$, который отправляет получателю.

Законный получатель приняв шифротекст *C*, расшифровывает его с помощью обратного преобразования $D_k=E_{k^{-1}}(C)$ и получает исходное сообщение в виде открытого текста *M*.

Преобразование E_k называется *криптоалгоритмом*.

Под *криптографическим ключом K* понимается конкретное секретное состояние некоторых параметров алгоритма криптографического преобразования данных, обеспечивающее выбор только одного варианта из всех возможных для данного алгоритма. Данный ключ, либо его часть, является закрытой информацией, которая должна быть известна только законным участникам криптографического обмена. Утеря секретной части ключа ведет к раскрытию всего защищенного обмена.

Криптоанализ

Любая попытка со стороны перехватчика расшифровать шифротекст *C* для получения открытого текста *M* или зашифровать свой собственный текст *M`* для получения правдоподобного шифротекста *C`*, не имея подлинного ключа, называется *криптоаналитической атакой*.

Если предпринятые криптоаналитические атаки не достигают поставленной цели и криптоаналитик не может, не имея подлинного ключа, вывести *M* из *C* или *C`* из *M`*, то систему называют *криптостойкой*.

Криптоанализ – это наука о раскрытии исходного текста зашифрованного сообщения без доступа к ключу. Успешный криптоанализ может раскрыть исходный текст или ключ.

Традиционные симметричные алгоритмы шифрования

Среди наиболее распространенных простейших алгоритмов шифрования информации можно выделить шифры перестановок и шифры замены (подстановки).

Шифрование перестановкой заключается в том, что символы шифруемого текста переставляются по определенному правилу в пределах некоторого блока этого текста.

Примерами шифров перестановки являются шифр «скитала», шифрующие таблицы.

Шифрование заменой (подстановкой) заключается в том, что символы шифруемого текста заменяются символами того же или другого алфавита в соответствие с заранее обусловленной схемой замены.

Примерами шифров замены являются моноалфавитная замена, многоалфавитная замена, шифр Цезаря, шифр Гросфельда, шифр Вижинера.

Система шифрования Цезаря

Шифр Цезаря является частным случаем шифра простой замены. Свое название этот шифр получил по имени римского императора Гая Юлия Цезаря, который использовал этот шифр при переписке с Цицероном (около 50 г. до н.э.).

При шифровании исходного текста методом Цезаря, каждая буква открытого текста заменяется на букву того же алфавита по следующему правилу. Заменяющая буква определяется путем смещения по алфавиту от исходной буквы на *K* букв (позиций). При достижении конца алфавита выполняется циклический переход к его началу. Смещение *K* в данном случае определяет ключ шифрования. Совокупность возможных подстановок для больших букв английского алфавита и *K*=3 представлена в таблице 1.

Таблица 1. Таблица подстановок

A	→	D		H	→	K		O	→	R		V	→	Y
B	→	E		I	→	L		P	→	S		W	→	Z
C	→	F		J	→	M		Q	→	T		X	→	A
D	→	G		K	→	N		R	→	U		Y	→	B
E	→	H		L	→	O		S	→	V		Z	→	C
F	→	I		M	→	P		T	→	W				
G	→	J		N	→	Q		U	→	X				

Математическая модель шифра Цезаря записывается в виде (1)

$$C=(P+K) \bmod M \quad (1)$$

где *C* – код символа шифротекста, *P* – код символа открытого текста, *K* – коэффициент сдвига, *M* – размер алфавита, mod – операция нахождения остатка от деления на *M*.

Например, результатом шифрования открытого текста RED APPLE по методу Цезаря с ключом *K*=3 будет являться последовательность UHG ASSOH.

Порядок выполнения лабораторной работы

1. Познакомиться на практике с демонстрационными моделями традиционных симметричных алгоритмов шифрования. Для этого запустить программу text12.exe от имени пользователя «Оля» пароль «123», запустить режим «Теория».
2. Пройти тестирование по изученному материалу, запустив в демонстрационной модели text12.exe режим «Тренаж».
3. Из таблицы 2 взять алгоритм шифрования и его ключ, соответствующие Вашему варианту. Реализовать программный модуль шифрования и дешифрования файлов на жестком диске ПК в соответствии с данным алгоритмом шифрования и ключом.
4. Оформить отчет по лабораторной работе.

Контрольные вопросы

1. Охарактеризуйте направление «криптография». Что называют криптографическим ключом?
2. Проклассифицируйте традиционные алгоритмы шифрования. Кратко охарактеризуйте эти классы.
3. Охарактеризуйте методы шифрования Цезаря, простую моноалфавитную замену, G-контурную многоалфавитную замену, простую перестановку, перестановки Гамильтона.
4. Что понимается под криптоанализом?

Таблица 1.1. Варианты

Вариант	Алгоритм шифрования	Ключ
1	Шифр Цезаря	K=4
2	Простая моноалфавитная замена	a=3, K=2
3	G-контурная многоалфавитная замена	K=33922
4	Простая перестановка	K=632514
5	Перестановки Гамильтона	K=13
6	Шифр Цезаря	K=2
7	Простая моноалфавитная замена	a=7, K=3
8	G-контурная многоалфавитная замена	K=12578
9	Простая перестановка	K=4172536
10	Перестановки Гамильтона	K=32
11	Шифр Цезаря	K=7
12	Простая моноалфавитная замена	a=11, K=2
13	G-контурная многоалфавитная замена	K=13243
14	Простая перестановка	K=32541
15	Перестановки Гамильтона	K=45
16	Шифр Цезаря	K=9
17	Простая моноалфавитная замена	a=13, K=5
18	G-контурная многоалфавитная замена	K=94827
19	Простая перестановка	K=813926457
20	Перестановки Гамильтона	K=14
21	Шифр Цезаря	K=8
22	Простая моноалфавитная замена	a=17, K=4
23	G-контурная многоалфавитная замена	K=37984
24	Простая перестановка	K=3124
25	Перестановки Гамильтона	K=35
26	Шифр Цезаря	K=11
27	Простая моноалфавитная замена	a=19, K=3
28	G-контурная многоалфавитная замена	K=2893475
29	Простая перестановка	K=35124
30	Перестановки Гамильтона	K=53

Пример оформления отчета по лабораторной работе

ЛАБОРАТОРНАЯ РАБОТА № 1
НАЗВАНИЕ ЛАБОРАТОРНОЙ РАБОТЫ

ВЫПОЛНИЛ: ст. гр. ….. ФИО
ВАРИАНТ № …

ЦЕЛЬ ЛАБОРАТОРНОЙ РАБОТЫ

В ходе выполнения лабораторной работы реализован алгоритм шифрования …… с ключом …..

КОД ПРОГРАММЫ

……..

РЕЗУЛЬТАТЫ РАБОТЫ ПРОГРАММЫ

Открытые данные …….
Результат шифрования …..
Результат дешифрования …..

4.2. Оценочные средства промежуточной аттестации

По дисциплине предусмотрен зачет. Зачет проходит по билетам. В каждом билете один теоретический вопрос и одно практическое задание. Зачет проводится в устной, письменной или компьютерной форме. Оценивается владение материалом, его системное освоение, способность применять нужные знания, навыки и умения при анализе проблемных ситуаций и решении практических заданий.

4.2.1. Устный или письменный ответ на вопрос

4.2.1.1. Порядок проведения и процедура оценивания.

Устный или письменный ответ на вопрос направлен на проверку знаний основных разделов информационной безопасности, основных защиты информации и криптографии.

4.2.1.2. Критерии оценивания.

«Отлично» ставится, если обучающийся:

В ответе качественно раскрыл содержание темы. Ответ хорошо структурирован. Прекрасно освоен понятийный аппарат. Продемонстрирован высокий уровень понимания материала. Превосходное умение формулировать свои мысли, обсуждать дискуссионные положения.

«Хорошо» ставится, если обучающийся:

Основные вопросы темы раскрыл. Структура ответа в целом адекватна теме. Хорошо освоен понятийный аппарат. Продемонстрирован хороший уровень понимания материала. Хорошее умение формулировать свои мысли, обсуждать дискуссионные положения.

«Удовлетворительно» ставится, если обучающийся:

Тему частично раскрыл. Ответ слабо структурирован. Понятийный аппарат освоен частично. Понимание отдельных положений из материала по теме. Удовлетворительное умение формулировать свои мысли, обсуждать дискуссионные положения.

«Неудовлетворительно» ставится, если обучающийся:

Тему не раскрыл. Понятийный аппарат освоен неудовлетворительно. Понимание материала фрагментарное или отсутствует. Неумение формулировать свои мысли, обсуждать дискуссионные положения.

4.2.1.3. Оценочные средства.

Вопросы для устного или письменного ответа

1. Основные понятия информационной безопасности.
2. Классификация угроз информационным системам. Неумышленные и умышленные угрозы.
3. Классификация угроз информационным системам (отказ в услуге, незаконное использование привилегий, "скрытые каналы", "маскарад", "сборка мусора", "люки").
4. Классификация угроз информационным системам (вредоносные программы: вирус, троянский конь, червяк, жадная программа, бактерия, логическая бомба, лазейки).
5. Основные методы обеспечения безопасности информационных систем. Правовое обеспечение безопасности.
6. Основные методы обеспечения безопасности информационных систем. Организационно-административное обеспечение.
7. Основные методы обеспечения безопасности информационных систем. Инженерно-технические меры обеспечения безопасности.
8. Основные методы обеспечения безопасности информационных систем. Основные функции технических средств подсистем безопасности.
9. Основные методы обеспечения безопасности информационных систем. Механизмы реализации функций технических средств подсистем безопасности.
10. Модели политик безопасности. Свободный и мандатный контроли за доступом.
11. Модели политик безопасности. Мандатные политики безопасности.
12. Модели политик безопасности. Модель Белла-Ла-Падулы.
13. Модели политик безопасности. Модель Биба.
14. Модели политик безопасности. Модель контроля целостности Кларка-Вилсона.
15. Модели политик безопасности. Политики избирательного разграничения доступа.
16. Идентификация и аутентификация субъектов.
17. Парольные системы идентификации и аутентификации пользователей. Основные требования к выбору и использованию паролей.
18. Парольные системы идентификации и аутентификации пользователей. Количественная оценка стойкости парольных систем.
19. Идентификация и аутентификация пользователей с использованием технических устройств.
20. Идентификация и аутентификация с использованием индивидуальных биометрических характеристик пользователя.
21. Криптографические методы защиты информации. Основные понятия криптографии.
22. Криптографические методы защиты информации. Классификация криптографических алгоритмов.
23. Криптоалгоритмы с ключом. Симметричные и асимметричные криптогалгоритмы.

24. Криптографические методы защиты информации. Виды атак на шифры.
25. Традиционные симметричные криптосистемы. Шифрование методом замены. Шифрование методом Цезаря.
26. Традиционные симметричные криптосистемы. Шифрование методом замены. Простая моноалфавитная замена.
27. Традиционные симметричные криптосистемы. Шифрование методом замены. Шифрующие таблицы Трисемуса.
28. Традиционные симметричные криптосистемы. Шифрование методом замены. Многооалфавитная замена. Шифр Гронсфельда.
29. Традиционные симметричные криптосистемы. Шифрование методом замены. Многооалфавитная замена. Система шифрования Вижинера.
30. Традиционные симметричные криптосистемы. Шифрование методом замены. Многооалфавитная замена. Шифрование методом Вернама.
31. Традиционные симметричные криптосистемы. Шифрование методом замены. Многооалфавитная замена. G-контурная многоалфавитная замена.
32. Традиционные симметричные криптосистемы. Шифрование методами перестановки. Метод простой перестановки.
33. Традиционные симметричные криптосистемы. Шифрование методами перестановки по маршрутам Гамильтона.
34. Традиционные симметричные криптосистемы. Шифрование методами перестановки. Шифрование методом гаммирования.

4.2.2. Практическое задание

4.2.2.1. Порядок проведения и процедура оценивания.

Предлагаются задачи на проверку умений проводить практические расчеты, анализировать полученные результаты; на владение навыками применения методов криптографии, правильно формировать выводы и заключения.

4.2.2.2. Критерии оценивания.

Оценка «отлично» ставится, если обучающийся:

Задание выполнено полностью и правильно.

Оценка «хорошо» ставится, если обучающийся:

Задание выполнено полностью, но нет достаточного обоснования. Или при верном решении допущена вычислительная ошибка или недочет, не влияющий на правильную последовательность рассуждений.

Оценка «удовлетворительно» ставится, если обучающийся:

Задание выполнено частично или с фактическими и вычислительными ошибками.

Оценка «неуцдовлетворительно» ставится, если обучающийся:

Задание не выполнено или выполнено с большим количеством фактических и вычислительных ошибок.

4.2.2.3. Оценочные средства.

1. Найдите ключ к "тарабарской грамоте" — тайнописи, применявшейся ранее в России для дипломатической переписки: "Пайцике тсюг т "камащамлтой чмароке" — кайпонили, нмирепяшвейля мапее ш Моллии цся цинсоракигелтой неменилти".
2. Дан русский текст и его построчный перевод на один инопланетный язык:
"Межпланетный корабль вызывает базу" - ом ку ра ля
"Сигнал корабля принят базой" - ку то ян ом
"Посадка просигналившего межпланетного корабля" - су то ку ля
Составьте фрагмент русско-инопланетного языка по этому переводу.
3. Робот придумал шифр для записи слов: заменил некоторые буквы алфавита однозначными или двузначными числами, используя только цифры 1, 2 и 3 (разные буквы он заменял разными числами). Сначала он записал шифром сам себя: РОБОТ = 3112131233. Зашифровав слова КРОКОДИЛ и БЕГЕМОТ, он с удивлением заметил, что числа вышли совершенно одинаковыми! Потом Робот записал слово МАТЕМАТИКА. Напишите число, которое у него получилось.
4. Как-то раз Света ехала в поезде. Чтобы не скучать, она стала зашифровывать названия разных городов, заменяя буквы их порядковыми номерами в алфавите. Когда Света зашифровала пункты прибытия и отправления поезда, то обнаружила, что они записываются с помощью всего лишь двух цифр: 21221-211221. Откуда и куда шёл поезд?
5. Ключом шифра, называемого «решетка», является трафарет, сделанный из квадратного листа клетчатой бумаги размером n×n (n — четно). Некоторые из клеток вырезаются с тем, чтобы в получившиеся отверстия на чистый лист бумаги того же размера можно было вписывать буквы текста, подлежащего зашифрованию. Одна из сторон трафарета является помеченной. Кроме того, трафарет должен обладать одним важным свойством: при наложении его на чистый лист бумаги четырьмя возможными способами (помеченной стороной вверх, вправо, вниз, влево) его вырезы полностью покрывают всю площадь квадрата, причем каждая клетка оказывается под вырезом ровно один раз.

Буквы сообщения, имеющего длину n2, последовательно вписываются в вырезы трафарета при каждом из четырех его указанных положений. После снятия трафарета на листе бумаги оказывается зашифрованное сообщение.
Найдите число различных ключей для произвольного четного числа n.
6. В адрес олимпиады пришла шифртелеграмма
ЦДОЗИФКДЦЮ·
Прочитайте зашифрованное сообщение, если известно, что использовался шифр, по которому к двузначному порядковому номеру буквы в алфавите (от 01 до 33) прибавлялось значение многочлена
f(x) = x6 + 3x5 + x4 + x3 + 4x2 + 4x + 5,
вычисленное либо при x = x1, либо при x = x2 (в случайном порядке), где x1,x2 — корни трехчлена x2 + 3x + 1, а затем полученное число заменялось соответствующей ему буквой.
7. Одна фирма предложила устройство для автоматической проверки пароля. Паролем может быть любой непустой упорядоченный набор букв в алфавите {a, b, c}. Будем обозначать такие наборы большими латинскими буквами. Устройство перерабатывает введенный в него набор P в набор Q = φ(P). Отображение φ держится в секрете, однако про него известно, что оно определено не для каждого набора букв P и обладает следующими свойствами. Для любого набора букв P
1) φ(aP) = P;
2) φ(bP) = φ(P)aφ(P);
3) набор φ(cP) получается из набора φ(P) выписыванием букв в обратном порядке.
Устройство признает предъявленный пароль верным, если φ(P) = P. Например, трехбуквенный набор bab является паролем, так как φ(bab) = φ(ab)aφ(ab) = bab. Подберите пароль, состоящий более, чем из трех букв.
8. Коммерсант для передачи цифровой информации с целью контроля передачи разбивает строчку передаваемых цифр на пятерки и после каждых двух пятерок приписывает две последние цифры от суммы чисел, изображенных этими пятерками. Затем процесс шифрования осуществляется путем прибавления к шифруемым цифрам членов арифметической прогрессии с последующей заменой сумм цифр остатками от деления на 10. Прочитайте зашифрованное сообщение:
4 2 3 4 6 1 4 0 5 3 1 3·
9. Рассмотрим модель шифра для цифрового текста, в котором каждая цифра заменяется остатком от деления значения многочлена
f(x) = b(x3 + 7x7 + 3x + a)
на число 10, где a,b — фиксированные натуральные числа. Выяснить, при каких значениях a и b возможно однозначное расшифрование.
10. Фирма предложила на рынок кодовый замок. При установке владелец замка сопоставляет каждой из 26 латинских букв, расположенных на клавиатуре, произвольное натуральное число (известное лишь обладателю замка). После выбора произвольной комбинации попарно различных букв, происходит суммирование числовых значений набранных букв и замок открывается, если сумма делится на 26. Докажите, что для любых числовых значений букв существует комбинация, открывающая замок.
11. Рассматривается шифр, в котором буквы русского 30-буквенного алфавита Ω занумерованы по следующей таблице:
А Б В Г Д Е Ж З И К Л М Н О П Р С Т У Ф Х Ц Ч Ш Щ Ь Ы Э Ю Я
1 2 3 4 5 6 7 8 9 10 11 12 13 14 15 16 17 18 19 20 21 22 23 24 25 26 27 28 29 30
Для зашифрования сообщения τ = t1t2...tn выбирается некоторая последовательность κ = γ1γ2...γn (ключ), состоящая из букв алфавита Ω. Зашифрование состоит в позначном сложении соответствующих букв из τ и κ с последующей заменой суммы буквой алфавита Ω, номер которой равен остатку от деления этой суммы на число 30.
Известно, что два сообщения τ1 и τ2 зашифрованы с помощью одного ключа (κ) и что каждое из них содержит слово «корабли». Восстановить τ1 и τ2 по текстам данных криптограмм:
σ1=ЮПТЦАРГШАЛЖЖЕВЦЩЫРВУУ
σ2=ЮПЯТБНЩМСДТЛЖГПСГХСЦЦ
8. Перехвачена «шифровка»: РБЬНПТСИТСРРЕЗОХ
Относительно шифра известно следующее:
— используется шифр предыдущей задачи;
— в качестве ключа используется произвольная последовательность, составленная из букв: А,Б,В.
Прочтите зашифрованное сообщение.
12. Шифр простой замены в алфавите A = {a1, a2,..., an}, состоящем из n различных букв, заключается в замене каждой буквы шифруемого текста буквой того же алфавита, причем разные буквы заменяются разными. Ключом шифра простой замены называется таблица, в которой указано, какой буквой надо заменить каждую букву алфавита A. Если слово СРОЧНО зашифровать простой заменой с помощью ключа:
АБВГДЕЖЗИКЛМНОПРСТУФХЦЧШЩЪЫЭЮЯ
ЧЯЮЭЫЫЦШЦХФУБДТЗВРПМЛКАИОЖЕСГН,

то получится слово ВЗДАБД. Зашифровав полученное слово с помощью того же ключа еще раз, получим новое слово ЮШЫЧЯЫ. Сколько всего различных слов можно получить, если указанный процесс шифрования продолжить неограниченно?

13. Сообщение, зашифрованное в пункте А шифром простой замены в алфавите из букв русского языка и знака пробела (_) между словами, передается в пункт Б отрезками по 12 символов. При передаче очередного отрезка сначала передаются все его знаки, стоящие на четных местах в порядке возрастания их номеров, начиная со второго, а затем — все знаки, стоящие на нечетных местах, также в порядке возрастания их номеров, начиная с первого. В пункте Б полученное шифрованное сообщение дополнительно шифруется с помощью некоторого другого шифра простой замены в том же алфавите, а затем таким же образом, как и из пункта А, передается в пункт В. По перехваченным в пункте В отрезкам:

СО_ГЖТПНБЛЖО
РСТКДКСПХЕУБ
_Е_ПФПУБ_ЮОБ
СП_ЕОКЖУУЛЖЛ
СМЦХБЭКГОЩПЫ
УЛКЛ_ИКНТЛЖГ,

восстановите исходное сообщение зная, что в одном из передаваемых отрезков зашифровано слово КРИПТОГРАФИЯ.

14. Дана последовательность C1, C2, C3, ..., Cn, ..., в которой Cn есть последняя цифра числа nn. Доказать, что эта последовательность периодическая и ее период равен 20.

15. Знаки алфавита, состоящего из букв русского языка и символа пробела между словами (_), заменим парами цифр согласно таблице:

А Б В Г Д Е Ж З И К Л М Н О П Р С Т У Ф Х Ц Ч Ш Щ Ь Ы Э Ю Я _
01 02 03 04 05 06 07 08 09 10 11 12 13 14 15 16 17 18 19 20 21 22 23 24 25 26 27 28 29 30 31

Для зашифрования сообщения длины m, записанного в этом алфавите, сначала преобразуем буквенный текст в цифровой T = t1, t2, ..., t2m,а затем, выбрав отрезок K = Cn+1, Cn+2, ..., Cn+2m последовательности из задачи 11, осуществим последовательное поразрядное сложение цифр текста T с цифрами отрезка K, причем в качестве очередного знака шифрованного текста берется цифра единиц соответствующей суммы (младший разряд).

Прочитайте зашифрованное сообщение:

2 3 3 9 8 6 7 2 1 6 4 5 8 1 6 0 6 7 0 6 1 7 3 1 5 5 8 8.

Приложение 2
к рабочей программе дисциплины (модуля)
Б1.В.04.06 Информационная безопасность

Перечень литературы, необходимой для освоения дисциплины (модуля)

Направление подготовки: 23.03.01 Технология транспортных процессов
Профиль подготовки: Проектирование и управление интеллектуальными транспортными системами
Квалификация выпускника: бакалавр
Форма обучения: заочное
Язык обучения: русский
Год начала обучения по образовательной программе: 2024

Основная литература:

1. Башлы, П. Н. Информационная безопасность и защита информации [Электронный ресурс]: учебник / П. Н. Башлы, А. В. Бабаш, Е. К. Баранова. - Москва: РИОР, 2013. - 222 с. - ISBN 978-5-369-01178-2. - Текст: электронный. - URL: https://znanium.com/catalog/product/405000. – Режим доступа: по подписке.
2. Гришина, Н. В. Информационная безопасность предприятия: Учебное пособие / Гришина Н.В., - 2-е изд., доп - Москва: Форум, НИЦ ИНФРА-М, 2016. - 240 с. (Высшее образование: Бакалавриат) (Обложка. КБС)ISBN 978-5-00091-007-8. - Текст: электронный. - URL: https://znanium.com/catalog/product/544554 – Режим доступа: по подписке.
3. Масленников, М. Е. Практическая криптография: Пособие / Масленников М.Е. - СПб:БХВ-Петербург, 2015. - 465 с. ISBN 978-5-9775-1884-0. - Текст: электронный. - URL: https://znanium.com/catalog/product/944503. – Режим доступа: по подписке.
4. Царев, Р.Ю. Информатика и программирование [Электронный ресурс] : учеб. пособие / Р. Ю. Царев, А. Н. Пупков, В. В. Самарин, Е. В. Мыльникова. - Красноярск: Сиб. федер. ун-т, 2014. - 132 с. - ISBN 978-5-7638-3008-8. - Текст: электронный. - URL: https://znanium.com/catalog/product/506203. – Режим доступа: по подписке.
5. Глинская, Е. В. Информационная безопасность конструкций ЭВМ и систем: Учебное пособие/ГлинскаяЕ.В., ЧичваринН.В. - Москва: НИЦ ИНФРА-М, 2016. - 118 с. (Высшее образование: Бакалавриат) ISBN 978-5-16-010961-9. - Текст: электронный. - URL: https://znanium.com/catalog/product/507334 – Режим доступа: по подписке.
6. Вышегуров, С. Х. Информатика [Электронный ресурс] : учеб. пособие / Новосиб. гос. аграр. ун-т. Агроном. фак.; сост.: И.И. Некрасова, С.Х. Вышегуров. - Новосибирск: Золотой колос, 2014. - 105 с. - Текст: электронный. - URL: https://znanium.com/catalog/product/516070. – Режим доступа: по подписке.

Приложение 3
к рабочей программе дисциплины (модуля)
Б1.В.04.06 Информационная безопасность

Перечень информационных технологий, используемых для освоения дисциплины (модуля), включая перечень программного обеспечения и информационных справочных систем

Направление подготовки: 23.03.01 Технология транспортных процессов
Профиль подготовки: Проектирование и управление интеллектуальными транспортными системами
Квалификация выпускника: бакалавр
Форма обучения: заочное
Язык обучения: русский
Год начала обучения по образовательной программе: 2024

Освоение дисциплины (модуля) предполагает использование следующего программного обеспечения и информационно-справочных систем:
1. Операционная система Microsoft office professional plus 2010, или Microsoft Windows 7 Профессиональная, или Windows XP (Volume License)
2. Пакет офисного программного обеспечения Microsoft Office 365, или Microsoft office professional plus 2010
3. Adobe Reader XI или Adobe Acrobat Reader DC
4. Браузер Mozilla Firefox
5. Браузер Google Chrome
6. Kaspersky Endpoint Security для Windows
7. Программная система для обнаружения текстовых заимствований в учебных и научных работах. АО «Антиплагиат»
8. Электронная библиотечная система «ZNANIUM.COM»
9. Электронная библиотечная система Издательства «Лань»
10. Электронная библиотечная система «Консультант студента»