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

2. Место дисциплины (модуля) в структуре ОПОП ВО

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

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)

4.2. Содержание дисциплины (модуля)

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

6. Фонд оценочных средств по дисциплине (модулю)

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

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

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

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

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

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

13. Приложение №1. Фонд оценочных средств

14. Приложение №2. Перечень литературы, необходимой для освоения дисциплины (модуля)

15. Приложение №3. Перечень информационных технологий, используемых для освоения дисциплины (модуля), включая перечень программного обеспечения и информационных справочных систем

Программу дисциплины разработал(а)(и) доцент, к.н., Галимуллина Э.З. (Кафедра математики и прикладной информатики),EZGalimullina@kpfu.ru

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
ОПК-10	Способен контролировать и обеспечивать производственную и экологическую безопасность на рабочих местах
ОПК-10.1	Знать методы контроля и обеспечения производственной и экологической безопасность на рабочих местах
ОПК-10.2	Уметь применять методы контроля и обеспечения производственной и экологической безопасность на рабочих местах
ОПК-10.3	Владеть навыками применения методов контроля и обеспечения производственной и экологической безопасность на рабочих местах

Обучающийся, освоивший дисциплину (модуль):

Должен знать:
основные методы контроля и обеспечения информационной безопасности в профессиональной сфере.

Должен уметь:
применять основные методы контроля и обеспечения информационной безопасности в профессиональной сфере.

Должен владеть:
навыками применения основных методов информационной безопасности в профессиональной сфере.

2. Место дисциплины (модуля) в структуре ОПОП ВО

Данная дисциплина (модуль) включена в Блок 1 "Дисциплины (модули)" Б1.О.05. основной профессиональной образовательной программы 15.03.06 «Мехатроника и робототехника» (Физические основы мехатроники и робототехники)" и относится к обязательной части.

Осваивается на 3 курсе в 5 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 76 часа(ов).

Контактная работа – 36 часа(ов), в том числе лекции - 18 часа(ов), практические занятия - 0 часа(ов), лабораторные работы - 18 часа(ов), контроль самостоятельной работы - 0 часа(ов).

Самостоятельная работа -36 часа(ов).

Контроль (зачёт / экзамен) - 0 часа(ов).

Форма промежуточного контроля дисциплины: зачетв 5 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.	5	2	0	0	
2.	Тема 2. Политики безопасности. Модели политик безопасности	5	2	0	2	10
3.	Тема 3. Стандарты информационной безопасности	5	6	0	0	10
4.	Тема 4. Криптографическая защита информации.	5	4	0	10	8
5.	Тема 5. Технологии аутентификации.	5	4	0	6	8
	Итого: 72 часа		18	0	18	36

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 (утвержденный приказом Министерства науки и высшего образования Российской Федерации от 6 апреля 2021 года № 245)

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" - https://omsu.ru/about/structure/science/ub/ISedokno/

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

Вид работ	Методические рекомендации
лекции	В ходе лекционных занятий следует вести конспектирование учебного материала. Обращать внимание на категории, формулировки, раскрывающие содержание темы, научные выводы и практические рекомендации. Желательно оставить в рабочих конспектах поля, на которых делать пометки из рекомендованной литературы, дополняющие материал прослушанной лекции, а также подчеркивающие особую важность тех или иных теоретических положений. Задавать преподавателю уточняющие вопросы с целью уяснения теоретических положений, практических рекомендаций, разрешения проблемных ситуаций. В ходе подготовки к лекционным занятиям повторить изложенный ранее учебный материал, ознакомиться с основной и дополнительной литературой, информацией из рекомендованных Интернет-ресурсов по изученной теме. Дорабатывать свой конспект лекции, делая в нем соответствующие записи из рекомендованной основной и дополнительной литературы, Интернет-ресурсов по проблемным вопросам.
лабораторные работы	Выполнение лабораторных работ направлено на обобщение, систематизацию, углубление теоретических знаний; формирование умений применять полученные знания в практической деятельности; развитие аналитических, проектировочных, конструктивных умений; выработку самостоятельности, ответственности и творческой инициативы. В ходе выполнения лабораторной работы студент должен проявить умение самостоятельно работать с учебной и научной литературой, Интернет-ресурсами, продемонстрировать навыки владения компьютерной техникой и пакетами прикладных программ соответствующего назначения. Контрольной точкой лабораторной работы является ее защита. Защита проводится в устной форме: студент должен уметь объяснить и обосновать каждый выполненный этап работы.
самостоя-тельная работа	Самостоятельная работа по данной дисциплине включает: повторение теоретического материала; подготовка к лабораторным занятиям; подготовка к тестированию и экзамену. Любая форма самостоятельной работы начинается с изучения конспекта лекции, соответствующей учебной и научной литературы, а также информации из рекомендованных Интернет-ресурсов. Во всех рекомендуемых учебниках и учебных пособиях содержатся контрольные вопросы, которые помогают повторить ключевые моменты соответствующей темы, и практические задания, нацеленные на выявление логических взаимосвязей.
зачет	зачет проводится в устной форме по билетам, в которых содержатся вопросы (задания) по всему разделу дисциплины. Оценивается владение теоретическим материалом, его системное освоение, взаимосвязь основных понятий дисциплины, способность применять знания и умения при решении практических заданий, приобретение навыков самостоятельной работы. Для подготовки к зачету рекомендуется повторить весь учебный материал по дисциплине, а также использовать основную и дополнительную литературу, информацию из рекомендованных Интернет-ресурсов.

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)

Материально-техническое обеспечение образовательного процесса по дисциплине (модулю) включает в себя следующие компоненты:

Учебная аудитория для проведения учебных занятий лекционного типа, семинарского типа, групповых и индивидуальных консультаций, текущего контроля и промежуточной аттестации № 61

Комплект мебели для преподавателя – 1 шт., посадочные места для обучающихся – 30 шт., одноместные столы – 12 шт., компьютерные столы – 18 шт., компьютеры – 19 шт., интерактивная панель – 1 шт., меловая доска

настенная – 1 шт., выход в интернет, внутривузовская компьютерная сеть, доступ в электронную информационно-образовательную среду.

Помещение для самостоятельной работы № 10

Посадочные места для пользователей – 28 шт., металлические двусторонние стеллажи для книг – 11 шт., книжный шкаф открытый – 5 шт., проектор – 1 шт., ноутбуки для пользователей – 11 шт., шкаф каталожный – 8 шт., шкаф для одежды – 1 шт., ксерокс – 1 шт., рабочий стол библиотекаря – 1 шт., компьютер библиотекаря – 1 шт., вешалка для одежды – 1 шт., жалюзи рулонные «Омега» с фотопечатью – 4 шт., стенд настенный (бронированное стекло) – 4 шт., шкаф-витрина встроенный в арку – 2 шт., шкаф-витрина стеклянный – 2 шт., стеллаж трубчатый с деревянными полками – 2 шт., рабочий стол для инвалидов и лиц с ОВЗ – 2 шт., стол СИ-1 рабочий для инвалидов-колясочников – 1 шт., компьютер– 2 шт., наушники – 2 шт., устройство «Говорящая книга» (тифлоплеер) – 2 шт., видеоувеличитель – 2 шт., радиокласс – 1 шт., портативный тактильный дисплей - 1 шт., сканирующая читающая машина - 1 шт., сканер – 1 шт., веб-камера – 1 шт., выход в интернет, внутривузовская компьютерная сеть, доступ в электронную информационно-образовательную среду.

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 15.03.06 «Мехатроника и робототехника» и профилю подготовки "Физические основы мехатроники и робототехники".

Приложение №1
к рабочей программе дисциплины (модуля)
Б1.О.05.07 Информационная безопасность

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

Фонд оценочных средств по дисциплине
Информационная безопасность

Направление подготовки: 15.03.06 Мехатроника и робототехника
Профиль подготовки: Физические основы мехатроники и робототехники
Квалификация выпускника: бакалавр
Форма обучения: очная
Язык обучения: русский
Год начала обучения по образовательной программе: 2025

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**
ОПК-10 Способен контролировать и обеспечивать производственную и экологическую безопасность на рабочих местах	Знать основные методы контроля и обеспечения информационной безопасности в профессиональной сфере. Уметь применять основные методы контроля и обеспечения информационной безопасности в профессиональной сфере. Владеть навыками применения основных методов информационной безопасности в профессиональной сфере.	**Текущий контроль:** *Тестирование* 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) (86-100 баллов)	**Средний уровень (хорошо) (71-85 баллов)**	**Низкий уровень (удовлетворительно) (56-70 баллов)**	**Ниже порогового уровня (неудовлетворительно) (0-55 баллов)**
ОПК-10	Знает основные методы контроля и обеспечения информационной безопасности в профессиональной сфере	Знает основные методы контроля и обеспечения информационной безопасности в профессиональной сфере. Допускает незначительные ошибки при ответе на вопрос или решении поставленной задачи	Знает основные методы контроля и обеспечения информационной безопасности в профессиональной сфере. Допускает типичные ошибки при ответе на вопрос или решении поставленной задачи	Не знает основные методы контроля и обеспечения информационной безопасности в профессиональной сфере.

	Умеет применять основные методы контроля и обеспечения информационной безопасности в профессиональной сфере	Умеет применять основные методы контроля и обеспечения информационной безопасности в профессиональной сфере. Допускает незначительные ошибки при ответе на вопрос или решении поставленной задачи	Умеет применять основные методы контроля и обеспечения информационной безопасности в профессиональной сфере. Допускает типичные ошибки при ответе на вопрос или решении поставленной задачи	Не умеет применять основные методы контроля и обеспечения информационной безопасности в профессиональной сфере
	Владеет навыками применения основных методов информационной безопасности в профессиональной сфере	Владеет навыками применения основных методов информационной безопасности в профессиональной сфере. Допускает незначительные ошибки при ответе на вопрос или решении поставленной задачи	Владеет навыками применения основных методов информационной безопасности в профессиональной сфере. Допускает типичные ошибки при ответе на вопрос или решении поставленной задачи	Не владеет навыками применения основных методов информационной безопасности в профессиональной сфере.

3. Распределение оценок за формы текущего контроля и промежуточную аттестацию

5 семестр:
Текущий контроль:
Тестирование. 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.
Максимальное количество баллов по БРС - 10.
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.
Максимальное количество баллов по БРС - 10.
Лабораторные работы. Тема 2. Политики безопасности. Модели политик безопасности. Тема 4. Криптографическая защита информации. Тема 5. Технологии аутентификации.
Максимальное количество баллов по БРС - 30.
Итого 10+10+30=50 баллов

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 экзамен обеспечивает случайное распределение вариантов экзаменационных 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.
Экзамен проводится по билетам. В каждом билете два оценочных средства: устный или письменный ответ на вопрос и решение задачи.

Устный или письменный ответ – 20 баллов.
Практическое задание – 30 баллов.
Итого 20+30=50 баллов.
Общее количество баллов по дисциплине за текущий контроль и промежуточную аттестацию: 50+50=100 баллов.

Соответствие баллов и оценок:
Для зачета:

56-100 баллов – зачтено
0-55 баллов – не зачтено

4. Оценочные средства, порядок их применения и критерии оценивания

4.1. Оценочные средства текущего контроля

4.1.1. Тестирование. 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.

Тестирование проходит в письменной форме или с использованием компьютерных средств. Обучающийся получает определённое количество тестовых заданий. На выполнение выделяется фиксированное время в зависимости от количества заданий. Оценка выставляется в зависимости от процента правильно выполненных заданий. Ниже приведены примерные задания.

4.1.1.2. Критерии оценивания

18-20 баллов ставится, если у обучающегося:
86% правильных ответов и более.
14-17 баллов ставится, если у обучающегося:
От 71% до 85 % правильных ответов.
11-13 баллов ставится, если у обучающегося:
От 56% до 70% правильных ответов.
0-10 баллов ставится, если у обучающегося:
55% правильных ответов и менее.

4.1.1.3. Содержание оценочного средства

Вариант 1

1. К основным преднамеренным искусственным угрозам АСОИ относится:
   а) пересылка данных по ошибочному адресу абонента
   б) физическое разрушение системы путем взрыва, поджога и т.п.
   в) неправомерное отключение оборудования или изменение режимов работы устройств и программ
   г) игнорирование организационных ограничений (установленных правил) при работе в системе
   д) разглашение, передача или утрата атрибутов разграничения доступа (паролей, ключей шифрования, идентификационных карточек, пропусков и т.п.).

2. В чем суть шифрования методом подстановки?
   а) символы шифруемого текста заменяются символами того же или другого алфавита в соответствие с заранее обусловленной схемой замены
   б) символы шифруемого текста последовательно складываются с символами некоторой специальной последовательности
   в) шифрование заключается в получении нового вектора как результата умножения матрицы на исходный вектор
   г) символы шифруемого текста заменяются другими символами, взятыми из одного или нескольких алфавитов
   д) замена слов и предложений исходной информации шифрованными

3. При шифрования методом перестановки ...
   а) символы шифруемого текста заменяются символами того же или другого алфавита в соответствие с заранее обусловленной схемой замены
   б) символы открытого текста переставляются по определенному правилу в пределах некоторого блока этого текста
   в) шифрование заключается в получении нового вектора как результата умножения матрицы на исходный вектор
   г) символы шифруемого текста заменяются другими символами, взятыми из одного или нескольких алфавитов
   д) замена слов и предложений исходной информации шифрованными

4. При шифрование методом гаммирования ...
   а) символы шифруемого текста заменяются символами того же или другого алфавита в соответствие с заранее обусловленной схемой замены
   б) символы открытого текста переставляются по определенному правилу в пределах некоторого блока этого текста
   в) наложение на открытые данные по определенному закону псевдослучайной последовательности, вырабатываемых по определенному алгоритму
   г) символы шифруемого текста заменяются другими символами, взятыми из одного или нескольких алфавитов
   д) замена слов и предложений исходной информации шифрованными

5. Символы шифруемого текста перемещаются по определенным правилам внутри шифруемого блока этого текста - это метод ...
   а) Гаммирования
   б) Подстановки
   в) Кодирования
   г) Перестановки
   д) Аналитических преобразований

6. Символы шифруемого текста последовательно складываются с символами некоторой специальной последовательности - это метод ...
   а) Гаммирования
   б) Подстановки
   в) Кодирования
   г) Перестановки
   д) Аналитических преобразований

7. Шифр DES - это ...
   а) система, которая предусматривает 3 режима шифрования (простая замена, гаммирование, гаммирование с обратной связью) и один режим выработки имитовставки
   б) система с открытым ключом предназначенная как для шифрования, так и для аутентификации основана на трудности разложения очень больших целых чисел на простые сомножители
   в) блочные шифры с ключом переменной длины, продукт экспортируется за пределы страны
   г) шифр состоящий из 64-битных повторяющихся блоков с 128-битным ключом и восемью проходами
   д) симметричный алгоритм шифрования, имеет блоки по 64 бит и основан на 16 кратной перестановке данных, для зашифровывания использует ключ в 56 бит.

8. Шифр RSA - это ...
   а) система, которая предусматривает 3 режима шифрования (простая замена, гаммирование, гаммирование с обратной связью) и один режим выработки имитовставки
   б) система с открытым ключом предназначенная как для шифрования, так и для аутентификации основана на трудности разложения очень больших целых чисел на простые сомножители
   в) блочные шифры с ключом переменной длины, продукт экспортируется за пределы страны
   г) шифр состоящий из 64-битных повторяющихся блоков с 128-битным ключом и восемью проходами
   д) симметричный алгоритм шифрования, имеет блоки по 64 бит и основан на 16 кратной перестановке данных, для зашифровывания использует ключ в 56 бит.

9. Шифр ГОСТ 28147-89 - это ...
   а) система, которая предусматривает 3 режима шифрования (простая замена, гаммирование, гаммирование с обратной связью) и один режим выработки имитовставки
   б) система с открытым ключом предназначенная как для шифрования, так и для аутентификации основана на трудности разложения очень больших целых чисел на простые сомножители
   в) блочные шифры с ключом переменной длины, продукт экспортируется за пределы страны
   г) шифр состоящий из 64-битных повторяющихся блоков с 128-битным ключом и восемью проходами

д) симметричный алгоритм шифрования, имеет блоки по 64 бит и основан на 16 кратной перестановке данных, для зашифровывания использует ключ в 56 бит.

10. Стандарт шифрования данных ГОСТ - это ...
а) 64 битовый блочный алгоритм с 256 битовым ключом
б) 64-битовый блочный алгоритм с 56 битовым ключом
в) блок данных представляется в виде двухмерного байтового массива размером 4X4, 4X6 или 4X8
г) 64-битовый блочный алгоритм с 48 битовым ключом

11. Какой ключ доступен всем для проверки ЭЦП?
а) Закрытый
б) Открытый
в) Внутренний
г) Приватный

12. Какие из следующих алгоритмов являются симметричными?
а) DES
б) Эль-Гамаль
в) RSA
г) AES
д) DSA
е) Гост 28147-89

13. Какая схема лежит в основе алгоритмов шифрования DES и ГОСТ 28147-89?
а) Цезаря
б) Кантора
в) Фейстеля
г) Вижинера
д) Эль-Гамаля

14. Как называется преобразование входного массива данных произвольной длины в выходную битовую строку фиксированной длины?
а) Разбиение входного массива
б) Сжатие
в) Хеширование

15. На какой труднорешаемой задаче основан алгоритм RSA?
а) Вычислении обратного элемента
б) Дискретного логарифмирования
в) Факторизации чисел
г) Нахождения большого простого числа

16. Что обычно в себя включает схема электронной подписи?
а) алгоритм генерации ключевых пар пользователя
б) функцию вычисления подписи
в) функцию проверки подписи
г) ничего из вышеперечисленного

17. В чем преимущество симметричных систем над асимметричными?
а) скорость шифрования
б) меньшая требуемая длина ключа для сопоставимой стойкости
в) простота обмена ключами
г) простота реализации
д) простота управления ключами в большой сети
е) все ответы правильные

18. Укажите виды симметричных криптосистем
   а) криптосистемы с открытым ключом
   б) поточные шифры
   в) блочные шифры
   г) ЭЦП

19. Симметричный алгоритм шифрования - это ...
   а) криптографический метод защиты информации, где для шифрования и дешифрования используется один и тот же ключ, сохранение которого в секрете обеспечивает надежность защиты
   б) метод защиты информации, где для шифрования используется открытый ключ, для дешифрования используется закрытый ключ
   в) преобразование, которое позволяет пользователям проверить авторство и подлинность
   г) метод защиты информации, где шифрование и дешифрование производят набором симметричных ключей

20. Асимметричный алгоритм шифрования - это ...
   а) метод защиты информации, где для шифрования и дешифрования информации используются различные ключи, причем ключи генерирует отправитель сообщения
   б) метод защиты информации, где для шифрования и дешифрования информации используются больше трех ключей
   в) метод защиты информации, где для шифрования и дешифрования информации используют астрономические методы
   г) метод защиты информации, где для шифрования и дешифрования информации используются различные ключи, причем ключи генерирует получатель сообщения

Ответы: 1-в, г, д; 2-а; 3-б; 4-в; 5-г; 6-а; 7-д; 8-б; 9-а; 10-а; 11-б; 12-а, г, е; 13-в; 14-в; 15-в; 16-б, в; 17-а, б, г; 18-б, в; 19-а; 20-г.

Вариант 2

1. Что понимают под понятием "закрытый ключ электронной цифровой подписи"?
   а) уникальная последовательность символов, известная владельцу сертификата ключа подписи и предназначенная для создания в электронных документах электронной цифровой подписи с использованием средств электронной цифровой подписи
   б) ключ электронной цифровой подписи, который зашифрован с помощью единственного симметричного ключа владельца
   в) уникальная последовательность символов, соответствующая закрытому ключу электронной цифровой подписи, доступная любому пользователю информационной системы и предназначенная для подтверждения с использованием средств электронной цифровой подписи подлинности электронной цифровой подписи в электронном документе
   г) ключ электронной цифровой подписи, которым шифруют заголовки электронных документов для установления подлинности владельца

2. Что такое открытый ключ электронной цифровой подписи?
   а) уникальная последовательность символов, соответствующая закрытому ключу электронной цифровой подписи, доступная любому пользователю информационной системы и предназначенная для подтверждения с использованием средств электронной цифровой подписи подлинности электронной цифровой подписи в электронном документе
   б) уникальная последовательность символов, известная владельцу сертификата ключа подписи и предназначенная для создания в электронных документах электронной цифровой подписи с использованием средств электронной цифровой подписи
   в) последовательность символов, изготавливаемая любым пользователем информационной системы по своему усмотрению, предназначенная для подтверждения с использованием средств электронной цифровой подписи подлинности электронной цифровой подписи в электронном документе
   г) ключ электронной цифровой подписи, которым шифруют заголовки электронных документов для установления подлинности владельца

3. Какие из представленных задач является примером однонаправленной функции?
   а) Вычисление обратного элемента
   б) Дискретного логарифмирования
   в) Факторизации чисел
   г) Нахождения большого простого числа
   д) Ни одна из представленных задач не является примером однонаправленной функции

4. В чем преимущество ассимметричных криптосистем?
   а) скорость шифрования
   б) меньшая требуемая длина ключа для сопоставимой стойкости
   в) простота обмена ключами
   г) простота реализации
   д) простота управления ключами в большой сети
   е) все ответы правильные

5. Какой из алгоритмов шифрования реализован на основе ассиметричных криптосистем на базе эллиптических кривых?
   а) ECES
   б) RSA
   в) DSA
   г) ГОСТ Р34.10-97

6. Какими свойства должна обладать функция хеширования?
   а) может быть применена к аргументу только определенной длины
   б) выходное значение хэш-функции имеет фиксированный размер
   в) хэш-функцию достаточно сложно вычислить для любого сообщения
   г) хэш-функция должна быть чувствительна к всевозможным изменениям в тексте
   д) хэш-функция должна быть однонаправленной
   е) вероятность того, что значения хэш-функций двух различных документов совпадут ничтожна мала
   ж) все варианты верные

7. В какой функции хэширования шифрование хранящегося в регистре хэш-значения происходит в виде четырех блоков по 64 бит в режиме простой замены?
   а) стандарт хэширования ГОСТ Р34.11-94
   б) стандарт хэширования MD
   в) стандарт хэширования DSA
   г) стандарт хэширования SHA

8. Что представляет собой электронная цифровая подпись?
   а) обычная рукописная подпись, только в электронном формате
   б) относительно небольшое количество дополнительной цифровой информации, передаваемой вместе с подписываемым текстом
   в) значение хэш-функции
   г) информация о лице подписавшего файл

9. Как называется режим шифрования блочных шифров, при котором каждый блок открытого текста перед шифрованием объединяется с помощью операции XOR с предыдущим блоком зашифрованного текста?
   а) Режим сцепления шифрованных блоков
   б) Режим шифрованной обратной связи
   в) Режим обратной связи по выходу
   г) Режим электронной шифровальной книги

10. Какова последовательность подписания сообщений с помощью ЭЦП?
   а) вычисляется хэш, затем хэш зашифровывается с помощью открытого ключа отправителя
   б) сообщение зашифровывается, после чего результат хэшируется

в) при подписании сообщение зашифровывается, при проверке вычисляется хэш
г) вычисляется хэш исходного сообщения, после чего оно зашифровывается с помощью закрытого ключа отправителя

11. Эллиптическая кривая имеет вид:
а) $y2 = x3 + ax + b \pmod p$
б) $y3 = x2 + ax + b \pmod p$
в) $y = x3 + ax2 + b \pmod p$
г) $x3 = y2 + ax + b \pmod p$

12. Чтобы расшифровать сообщение с помощью асимметричного алгоритма шифрования используются:
а) открытый ключ отправителя
б) открытый ключ получателя
в) закрытый ключ отправителя
г) закрытый ключ получателя

13. Какова последовательность проверки подлинности полученного сообщения с ЭЦП?
а) ЭЦП расшифровывается открытым ключом отправителя и вычисляется хэш полученного сообщения
б) ЭЦП расшифровывается открытым ключом получателя и вычисляется хэш полученного сообщения
в) вычисляется обратная функция хэш-функции и проверяется подлинность ЭЦП
г) ЭЦП расшифровывается закрытым ключом получателя и вычисляется хэш полученного сообщения

14. Какой алгоритм хэширования используется для защиты баз данных аутентификации в ОС?
а) алгоритм хэширования LANMAN
б) алгоритм хэширования NTLM
в) алгоритм хэширования RSA
г) алгоритм хэширования ГОСТ

15. Что относят к преимуществам защиты пристыковочного типа?
а) простота тиражирования программных систем защиты
б) простота технологии применения
в) не требует наличия исходных текстов программы
г) имеются элементы защиты ПО от изучения с помощью отладчиков и дизассемблеров
д) более просто реализовать любую реакцию системы защиты ПО на несанкционированный запуск
е) можно опрашивать идентифицирующий элемент где угодно, когда угодно и столько раз, сколько нужно

16. Какие действия выполняются в режиме шифрования простой замены?
а) зашифрование каждого 64-бит блока информации выполняются 32 описанных раунда
б) каждый блок открытого текста побитно складывается по модулю 2 с блоком гаммы шифра размером 64 бит
в) для заполнения регистров N1 и N2, с обратной связью начиная со 2-го блока, используется не предыдущий блок гаммы, а результат зашифрования предыдущего блока открытого текста
г) первый 64-бит блок массива информации, для которого вычисляется криптографическая контрольная сумма, записывается в регистры N1 и N2 и зашифровывается в сокращенном режиме

17. Какая категория является наиболее рискованной для компании с точки зрения вероятного мошенничества и нарушения безопасности?
а) сотрудники
б) хакеры
в) атакующие
г) контрагенты (лица, работающие по договору)

18. Если различным группам пользователей с различным уровнем доступа требуется доступ к одной и той же информации, какое из указанных ниже действий следует предпринять руководству?

а) снизить уровень безопасности этой информации для обеспечения ее доступности и удобства использования

б) требовать подписания специального разрешения каждый раз, когда человеку требуется доступ к этой информации

в) улучшить контроль за безопасностью этой информации

г) снизить уровень классификации этой информации

19. Кто в конечном счете несет ответственность за гарантии того, что данные классифицированы и защищены?

а) владельцы данных

б) пользователи

в) администраторы

г) руководство

20. Когда целесообразно не предпринимать никаких действий в отношении выявленных рисков?

а) никогда.

б) когда риски не могут быть приняты во внимание по политическим соображениям

в) когда необходимые защитные меры слишком сложны

г) когда стоимость контрмер превышает ценность актива и потенциальные потери

Ответы: 1-а; 2-а; 3-б, в; 4-в, д; 5-а; 6-а, г, д, е; 7-а; 8-б; 9-а; 10-г; 11-а; 12-в; 13-а; 14-а, б; 15-а, б, в, г; 16-а; 17-а; 18-в; 19-г; 20-г

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 проведенияи 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.

Требования к реферату

При оформлении текста реферата следует придерживаться следующих параметров:

поля: левое – 35 мм, правое – 15 мм, верхнее – 25 мм, нижнее – 25 мм;

ориентация страницы: книжная;

шрифт: TimesNewRoman;

кегль: 14 пт (пунктов);

красная строка:1 мм;

междустрочный интервал: полуторный;

выравнивание основного текста и сносок: по ширине.

Иллюстрации в виде рисунков, фотоснимков, схем и т.п. могут располагаться органично с текстом (возможно ближе к иллюстрируемой части) либо на отдельных листах. В любом случае выполняется нумерация (сквозная для всех разделов), которая располагается вверху. Подрисуночную нумерацию и надпись располагать внизу.

Заканчивается пояснительная записка библиографическим списком источников, к которым обращался студент во время работы над разрабатываемой темой.

Объем информационно-технологической документации не регламентируется – он диктуется достаточностью для практического применения. Карточки задания для самоконтроля (если таковы имеются) вкладываются в прозрачные файлы.

Реферат по своему структурному содержанию должен содержать следующие элементы:

- титульный лист;
- содержание;
- введение;
- базовое понятия;
- историческая справка (особенности зарождения и развития, основоположники и т.д.);
- классификация (виды, формы и т.д.);
- общее и частное положения по применению в учебно-воспитательном процессе;

- глоссарий;
- список использованных источников
- приложения

4.1.2.2 Критерии оценивания

9-10 баллов 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.

7-8 баллов 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.

5-6 баллов 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.

0-4 балла 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 NovellNetWare
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.

В аудитории, оснащённой соответствующим оборудованием, обучающиеся проводят учебные эксперименты и тренируются в применении практико-ориентированных технологий. Оцениваются знание материала и умение применять его на практике, умения и навыки по работе с оборудованием в соответствующей предметной области.

Лабораторные работы проводятся преподавателем согласно разработанному и утвержденному на кафедре рабочей программе. Каждая лабораторно-практическая работа выполняется по определенной теме программы в соответствии с заданием.

Перед выполнением каждой работы студенты-бакалавры должны проработать соответствующий материал, используя конспекты теоретических занятий, периодические издания, учебно-методические пособия и учебники

На каждом занятии студенты выполняют работу в соответствии с ее содержанием и методическими указаниями.

По окончании занятий студенты оформляют отчет по каждой работе, соблюдая следующую форму:

- Наименование темы;
- Цель работы;
- Задание и содержание выполненной работы,
- Письменные ответы на контрольные вопросы.
- Выводы по проделанной работе.
- Список использованных источников.

4.1.3.2 Критерии оценивания

26-30 баллов ставится, если обучающийся:
Правильно выполнил все задания. Продемонстрировал высокий уровень владения материалом. Проявлены превосходные способности применять знания и умения к выполнению конкретных заданий.
21-25 баллов 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.
17-20 баллов 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.
0-16 баллов 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

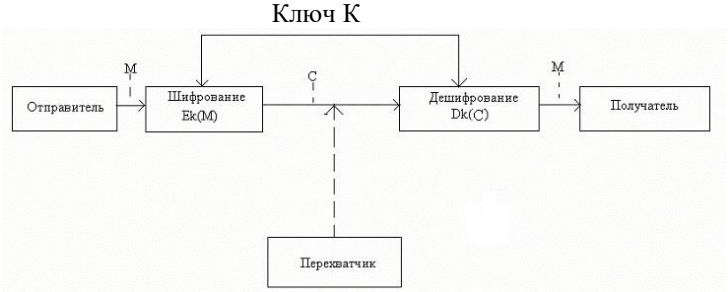
Темы 2, 4, 5
Лабораторная работа 1 «Методы криптографической защиты информации. Простейшие алгоритмы шифрования (Система шифрования Цезаря, Простая моноалфавитная замена, G-контурная многоалфавитная замена, Простая перестановка, Перестановки Гамильтона)».
Лабораторная работа 2 «Элементы криптоанализа. 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:



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 *шифротекстC*=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 REDAPPLE по методу Цезаря с ключомK=3 будет являться последовательность UHGASSOH.

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 экзамен. Экзамен проходит по билетам. В каждом билете один теоретический вопрос и однопрактическое задание. Экзамен 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 проведенияи 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.

17-20 баллов 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.

14-16 баллов 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.

11-15 баллов 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.

0--10 баллов 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.

Краткие ответы:

1. Основные понятия информационной безопасности

Разговор об информационной безопасности необходимо начать с самого объекта защиты. Если говорить о термине «информация», то для него существует масса определений. Так, например, в Законе РФ «Об информации, информатизации и защите информации» принято следующее определение: « Под информацией понимаются сведения о лицах, предметах, фактах, событиях, явлениях и процессах независимо от формы их представления».

Информация имеет несколько категорий, таких как адекватность, достоверность, полнота, избыточность, объективность, актуальность. Если же исходить с точки зрения информационной безопасности, то информация должна обладать следующими категориями:

- конфиденциальность – гарантия того, что конкретная информация доступна только тем пользователям, которым этот доступ разрешен (авторизованным пользователям);
- целостность – гарантия сохранения за информацией правильных значений, не измененных в процессе хранения и передачи;
- аутентичность – гарантия того, что источником информации является именно то лицо, которое заявлено как ее автор;
- апеллируемость – гарантия того, что информацию можно привязать к ее автору и при необходимости доказать, что автором сообщения является именно заявленный человек, и не может являться никто другой;
- доступность – гарантия того, что авторизованные пользователи всегда смогут получить доступ к информации.

Таким образом, главной задачей подсистемы безопасности информационной системы является обеспечения указанных категорий информации. Под информационной безопасностью будем понимать защищенность информации и поддерживающей инфраструктуры (совокупности программных и аппаратных средств, обеспечивающих хранение, обработку и передачу информации) от случайных или преднамеренных воздействий естественного или искусственного характера, которые могут нанести неприемлемый ущерб субъектам информационных отношений, в том числе владельцам и пользователям информации и поддерживающей инфраструктуры. Защита информации – это комплекс мероприятий, направленных на обеспечение информационной безопасности.

2. Классификация угроз информационным системам. Неумышленные и умышленные угрозы

Под угрозой будем понимать потенциально возможные воздействия на систему, которые прямо или косвенно могут нанести урон пользователю. Непосредственную реализацию угрозы называют атакой.

Знание возможных угроз, а также уязвимых мест защиты, которые эти угрозы обычно эксплуатируют, необходимо для того, чтобы выбирать наиболее экономичные средства обеспечения безопасности.

Имеет смысл различать неумышленные и умышленные угрозы.

Неумышленные угрозы связаны с:

- ошибками оборудования или программного обеспечения: сбои процессора, питания, нечитаемые дискеты, ошибки в коммуникациях, ошибки в программах;
- ошибками человека: некорректный ввод, неправильная монтировка дисков, запуск неправильных программ, потеря дисков, пересылка данных по неверному адресу;
- форс-мажорными обстоятельствами.

Умышленные угрозы, в отличие от случайных, преследуют цель нанесения ущерба пользователям информационных систем и, в свою очередь, подразделяются на активные и пассивные. Пассивная угроза - несанкционированный доступ к информации без изменения состояния системы, активная – связана с попытками перехвата и изменения информации.

3. Классификация угроз информационным системам (отказ в услуге, незаконное использование привилегий, «скрытые каналы», «маскарад», «сборка мусора», «люки»)

К наиболее распространенным угрозам безопасности относят:

Несанкционированный доступ (НСД) – наиболее распространенный вид компьютерных нарушений. Он заключается в получении пользователем доступа к ресурсу, на который у него нет разрешения в соответствии с принятой в организации политикой безопасности.

Отказ в услуге. Представляет собой преднамеренную блокировку легального доступа к информации и другим ресурсам;

Незаконное использование привилегий. Злоумышленники, применяющие данный способ атаки, обычно используют штатное программное обеспечение, функционирующее в нештатном режиме. Незаконный захват привилегий возможен либо при наличии ошибок в самой системе, либо в случае халатности при управлении системой. Строгое соблюдение правил управления системой защиты, соблюдение принципа минимума привилегий позволяет избежать таких нарушений.

«Скрытые каналы». Представляют собой пути передачи информации между процессами системы, нарушающие системную политику безопасности. В среде с разделением доступа к информации пользователь может не получить разрешение на обработку интересующих его данных, однако может придумать для этого обходные пути. «Скрытые каналы» могут быть реализованы различными путями, в частности при помощи программных закладок («троянских коней»).

«Маскарад». Под «маскарадом» понимается выполнение каких-либо действий одним пользователем от имени другого пользователя. Такие действия другому пользователю могут быть разрешены. Нарушение заключается в присвоении прав и привилегий.

«Сборка мусора». После окончания работы обрабатываемая информация не всегда полностью удаляется из памяти ПК. Данные хранятся на носителе до перезаписи или уничтожения; при выполнении этих действий на освободившемся пространстве диска находятся их остатки. При искажении заголовка файла их прочитать трудно, но все же возможно с помощью специальных программ и оборудования. Такой процесс принято называть «сборкой мусора». Он может привести к утечке важной информации.

«Люки». Представляют собой скрытую, недокументированную точку входа в программный модуль. «Люки» относятся к категории угроз, возникающих вследствие ошибок реализации какого-либо проекта (системы в целом, комплекса программ и т. д.). Поэтому в большинстве случаев обнаружение «люков» – результат случайного поиска.

4. Классификация угроз информационным системам (вредоносные программы: вирус, троянский конь, червяк, жадная программа, бактерия, логическая бомба, лазейки)

Вредоносные программы. В последнее время участились случаи воздействия на вычислительную систему специально созданными программами. Для обозначения всех программ такого рода был предложен термин «вредоносные программы». Эти программы прямо или косвенно дезорганизуют процесс обработки информации или способствуют утечке или искажению информации. К самым распространенным видам подобных программ относятся:

«Вирус»– это программа, которая способна заражать другие программы, модифицируя их так, чтобы они включали в себя копию вируса.

«Троянский конь» – программа, которая содержит скрытый или явный программный код, при исполнении которого нарушается функционирование системы безопасности. «Троянские кони» способны раскрыть, изменить или уничтожить данные или файлы. Их встраивают в программы широкого пользования, например, в программы обслуживания сети, электронной почты.

«Червяк» – программа, распространяемая в системах и сетях по линиям связи. Такие программы подобны вирусам: заражают другие программы, а отличаются от вирусов тем, что не способны самовоспроизводиться.

«Жадная» программа – программа, которая захватывает (монополизирует) отдельные ресурсы вычислительной системы, не давая другим программам возможности их использовать.

«Бактерия» – программа, которая делает копии самой себя и становится паразитом, перегружая память ПК и процессор.

«Логическая бомба»– программа, приводящая к повреждению файлов или компьютеров (от искажения данных – до полного уничтожения данных). «Логическую бомбу» вставляют, как правило, во время разработки программы, а срабатывает она при выполнении некоторого условия (время, дата, ввода кодового слова).

«Лазейки» – точка входа в программу, благодаря которой открывается доступ к некоторым системным функциям. Обнаруживается путем анализа работы программы.

5. Основные методы обеспечения безопасности информационных систем. Правовое обеспечение безопасности

Для того, чтобы противостоять перечисленным в предыдущей главе угрозам, современные информационные системы включают в себя подсистемы безопасности, которые реализуют принятую политику безопасности. Политика безопасности в зависимости от целей и условий функционирования системы может определять права доступа субъектов к ресурсам, регламентировать порядок аудита действий пользователей в системе, защиты сетевых коммуникаций, формулировать способы восстановления системы после случайных сбоев и т.д. Для реализации принятой политики безопасности существуют правовые, организационно-административные и инженерно-технические меры защиты информации.

Правовое обеспечение безопасности информации – это совокупность законодательных актов, нормативно-правовых документов, положений, инструкций, руководств, требования которых обязательны в системе защиты информации. В нашей стране правовые основы обеспечения безопасности компьютерных систем составляют: Конституция РФ, Законы РФ, Кодексы (в том числе Уголовный Кодекс), указы и другие нормативные акты. Так, например, Уголовный Кодекс содержит главу 28, которая называется «Преступления в сфере компьютерной безопасности» и содержит описание состава компьютерных преступлений, подлежащих уголовному преследованию и полагающиеся наказания.

6. Основные методы обеспечения безопасности информационных систем. Организационно-административное обеспечение

Организационно-административное обеспечение безопасности информации представляет собой регламентацию производственной деятельности и взаимоотношений исполнителей на нормативно-правовой основе таким образом, чтобы разглашение, утечка и несанкционированный доступ к информации становился невозможным или существенно затруднялся за счет проведения организационных мероприятий. К мерам этого класса можно отнести: подбор и обучение персонала, определение должностных инструкций работников, организацию пропускного режима, охрану помещений, организацию защиты информации с проведением контроля работы персонала с информацией, определение порядка хранения, резервирования, уничтожения конфиденциальной информации и т.п.

7. Основные методы обеспечения безопасности информационных систем. Инженерно-технические меры обеспечения безопасности

Инженерно-технические меры представляют собой совокупность специальных органов, технических средств и мероприятий, функционирующих совместно для выполнения определенной задачи по защите информации. К инженерным средствам относят экранирование помещений, организация сигнализации, охрана помещений с ПК.

8. Основные методы обеспечения безопасности информационных систем. Основные функции технических средств подсистем безопасности

Технические средства защиты включают в себя аппаратные, программные, криптографические средства защиты, которые затрудняют возможность атаки, помогают обнаружить факт ее возникновения, избавиться от последствий атаки.

Технические средства подсистем безопасности современных распределенных информационных систем выполняют следующие основные функции:

- аутентификация партнеров по взаимодействию, позволяющая убедиться в подлинности партнера при установлении соединения;
- аутентификация источника информации, позволяющая убедиться в подлинности источника сообщения;
- управление доступом, обеспечивающее защиту от несанкционированного использования ресурсов;
- конфиденциальность данных, которая обеспечивает защиту от несанкционированного получения информации;
- целостность данных, позволяющая обнаружить, а в некоторых случаях и предотвратить изменение информации при ее хранении и передаче;
- принадлежность, которая обеспечивает доказательство принадлежности информации определенному лицу.

9. Основные методы обеспечения безопасности информационных систем. Механизмы реализации функций технических средств подсистем безопасности

Для реализации указанных функций используются следующие механизмы:

- шифрование, преобразующее информацию в форму, недоступную для понимания неавторизованными пользователями (подробнее шифрование рассматривается в главе 2);
- электронная цифровая подпись, переносящая свойства реальной подписи на электронные документы (подробнее см. гл.4);
- механизмы управления доступом, которые управляют процессом доступа к ресурсам пользователей на основе такой информации как базы данных управления доступом, пароли, метки безопасности, время доступа, маршрут доступа, длительность доступа;
- механизмы контроля целостности, контролирующие целостность как отдельного сообщения, так и потока сообщений и использующие для этого контрольные суммы, специальные метки, порядковые номера сообщений, криптографические методы;
- механизмы аутентификации, которые на основании предъявляемых пользователем паролей, аутентифицирующих устройств или его биометрических параметров принимают решение о том, является ли пользователь тем, за кого себя выдает;
- механизмы дополнения трафика, добавляющие в поток сообщений дополнительную информацию, «маскирующую» от злоумышленника полезную информацию;
- механизмы нотаризации, которые служат для заверения подлинности источника информации.

10. Модели политик безопасности. Свободный и мандатный контроли за доступом

С самого начала компьютерной эры одной из основных задач для разработчиков информационных технологий стала задача обеспечения безопасности. Ни одна существующая коммерческая или государственная электронная система не может обходится без защиты собственной информации от несанкционированного доступа. Начиная с 70-х годов прошлого века в мире стали разрабатываться различные концепции и методы защиты информации, что вскоре привело к созданию единообразного подхода к этой проблеме: были разработаны первые политики безопасности.

Политика безопасности – свод формальных правил, определяющих обработку, распространение и защиту информации.

Модель политики безопасности – формальное представление политики безопасности для определенной системы или класса систем, определяющее методы обработки, распространения и защиты информации.

Общие принципы:

Формальные правила в большинстве моделей определяют следующие требования в порядке важности:

1) Доступность

2)Целостность

3)Конфиденциальность

4)Подотчетность

Каждое из требований отвечает за свою область в модели политики безопасности:

Доступность – требование, отвечающее за доступ к информации, а именно:

• Предоставление доступа легальным пользователям в разрешенных масштабах.

• Предотвращение отсутствия такового.

• Предотвращение от нелегального доступа.

Целостность отвечает за две области:

• Целостность информации – обеспечение защиты информации от нелегальных действий в процессе хранения, обработки и передачи.

• Целостность системы – отсутствие двойственности в работе системы.

Конфиденциальность – требование к защищенности личной и секретной информации, применяется к данным в процессе хранения, обработки и передачи. Является наиболее важным требованием для некоторых типов данных или систем, таких, как секретный ключ или сервер аутентификации.

Подотчетность – требование, по которому любое действие можно было бы проследить от начала и до конца. Позволяет обнаружить нелегальное использование системы, обеспечивает защиту систем от ошибок и восстановление системы в случае их возникновения.

Все эти требования, в конечном счете, и формируют защищенность, которую в каждом отдельном случае следует понимать лишь как определенный набор требований к вышеизложенным целям.

Помимо набора требований одним из важнейших атрибутов модели, непосредственно влияющих на её реализацию, являются предусмотренные в модели методы контроля за доступом к системе. Большинство защищенных методов контроля за доступом к системе делятся на два класса:

• Свободный (самостоятельный) контроль за доступом в систему (Discretionary Access Control) является свободным в том смысле, что владелец или распорядитель информации может самостоятельно менять возможности доступа к своей информации. Характерен для моделей, предназначенных для реализации в коммерческих и научных целях.

• Мандатный контроль за доступом (Mandatory Access Control) в систему означает независимость доступности информации от её владельца. Как правило в подобных случаях контроль за доступом реализуется исходя из свойств самой информации и свойств желающего получить к ней доступ согласно независимым от них обоих правилам. Характерен для моделей, предназначенных для реализации в военных и государственных системах защиты.

Строго говоря критерии определения того, к какому классу относится тот или иной метод контроля за доступом, далеко не всегда дают определенный результат, но являются весьма точными для большинства классических моделей политики безопасности.

В 80-х годах под руководством Министерство обороны США (Department of Defense) разработало первый документ, определяющий систему стандартов в области компьютерной безопасности – “Критерии оценки безопасности компьютерных систем”

(The Trusted Computer System Evaluation Criteria), который чаще называют “Оранжевой книгой”. В частности этот документ содержит классификацию систем безопасности согласно строгости требований к безопасности, заложенных в их модели политики безопасности. В настоящий момент стандарты компьютерной безопасности определяются более чем десятком документов.

11. Модели политик безопасности. Мандатные политики безопасности

Мандатные модели управления доступом были созданы по результатам анализа правил секретного документооборота, принятых в государственных и правительственных учреждениях многих стран.

Исходная мандатная политика безопасности строится на базе следующей совокупности аксиом, определяющих правило разграничения доступа субъектов к обрабатываемой информации:

1. Вводится множество атрибутов (уровней) безопасности А, элементы которого упорядочены с помощью установленного отношения доминирования. Например, для России характерно использование следующего множества уровней безопасности А={открыто (О), конфиденциально (К), секретно (С), совершенно секретно (СС), особая важность (ОВ)}.

2. Каждому объекту компьютерной системы ставится в соответствие атрибут безопасности, который соответствует ценности объекта и называется его уровнем (грифом) конфиденциальности.

3. Каждому субъекту компьютерной системы ставится в соответствие атрибут безопасности, который называется уровнем допуска субъекта и равен максимальному из уровней конфиденциальности объектов, к которому субъект будет иметь допуск.

4. Если субъект имеет уровень допуска, а объект имеет уровень конфиденциальности , то будет иметь допуск к тогда и только тогда, когда .

Основным недостатком исходной мандатной политики безопасности является то, что в ней не различаются типы доступа вида «чтение» и «запись». Это создает потенциальную возможность утечки информации сверху вниз, например, путем запуска в компьютерной системе программной закладки с максимальным уровнем допуска, способной записывать информацию из объектов с верхних уровней конфиденциальности в объекты с более низкими уровнями, откуда она может быть прочитана субъектами с низким уровнем допуска.

12. Модели политик безопасности. Модель Белла-Ла-Падулы

Первой моделью системы безопасности стала модель Белла - Ла-Падулы (Bell-LaPadula model), созданная в 1973-74 годах в MITRE в городе Белфорде в штате Массачусетс по заказу Военно-Воздушных сил США. В 76 году была дополнена до использования в пределах концепции MULTICS (информационно-вычислительная система с мультиплексированием каналов передачи данных), в 86 году адаптирована для использования в сетевых системах. На протяжении 70-х годов оставалась главной моделью политики безопастности и оказала значительное влияние на формирование TCSEC. В изначальном варианте модель Белла – Ла-Падулы предусматривала возможность только мандатный контроль за доступом.

13. Модели политик безопасности. Модель Биба

Последующим расширением модели Белла - Ла-Палуды стала модель Биба (Biba Model), разработанная в 1977 году. Целью создания модели стало добавление в модель Белла - Ла-Палуды целостности. Задача была реализована путем добавления к субъектам и объектам уровня целостности и запрета общения субъектов и объектов разных уровней.

Для дополнительного управления целостностью введены понижающие водяные знаки (нарушающие запрет на общение):

• Если субъект читает объект более низкого уровня, то его уровень целостности снижается до уровня целостности объекта.

• Если субъект дополняет объект более высокого уровня, то уровень целостности объекта снижается до уровня целостности субъекта.

Модель не только несет в себе достоинства и недостатки модели Белла – Ла-Палуды, но и добавляет собственные: основной недостаток модели состоит в том, что введение уровней целостности только ограничивает возможности доступа субъектов к объектам, создавая либо значительную изоляцию между уровнями целостности, либо после определения уровней целостности этот уровень может только понижаться, что само по себе лишает его управляемости, и как следствие функциональности. Область применения модели Биба так же не выходит за пределы военных организаций.

14. Модели политик безопасности. Модель контроля целостности Кларка-Вилсона

Десять лет спустя была разработана модель Кларка-Вилсона (Clark-Wilson model), обеспечивающая требование целостности более практичным методом. В 1993 году модель была расширена и включила в себя разделение обязанностей. Основной областью применения данной модели является коммерция, в частности банковское дело.

В основе концепции модели стоят 2 принципа:

• Внутренняя целостность – свойства внутреннего состояния системы, достигаемые посредством “Правильных соглашений”.

• Внешняя целостность – взаимодействие внутреннего состояния системы с внешнем миром, реализуемая посредством разделение обязанностей.

Модель реализована посредством набора правил, и, в отличие от предыдущих моделей, не является математически формализованной моделью. Также субъекты теперь не имеют прямого доступа к объектам, между субъектом и объектом находится “слой” программ, которые обладает доступом к объектам. Контроль за доступом к системе является свободным.

Контроль за доступом к данным разделен на 2 группы:

• Определяются операции доступа, которые можно производить над каждым типом данных (только определенный набор программ имеет доступ к определенным объектам).

• Определяются операции доступа, которые могут быть произведены определенным субъектом (субъект имеет доступ только к определенному набору программ).

Все данные в модели Кларка-Вилсона разделены на 2 класса:

• Необходимый элемент данных (CDI)

• Спонтанный элемент данных (UDI)

Далее устанавливается набор правил, регулирующих взаимодействие с обоими типами данных (Certification Rules):

• Все начальные процедуры проверки (IVP) должны убедиться в том, что все CDI находятся в достоверном состоянии во время работы IVP.

• Все процедуры изменения (TP)должны быть сертифицированы, чтобы быть достоверными, т.е. все достоверные CDI должны переходить в достоверные CDI, причем каждая процедура изменения имеют право на доступ только к определенному набору CDI.

• Правила доступа должны удовлетворять всем требованиям разделения обязанностей.

• Все процедуры изменения должны быть записаны в доступный только-на-добавление журнал.

• Любая процедура изменения, получившая на вход UDI должна либо преобразовать его в CDI, либо отменить операцию.

Этот набор правил позволяет обеспечить работу с данными в таком режиме, когда полностью обеспечена безопасность и подотчетность переходов в системе. Главное достижение этих правил по сравнению с моделью Биба – разделение процедур по проверке целостности и процедур изменения. Позволяет предотвратить или исправить большинство нелегальных действий, совершаемых изнутри коммерческой организации.

15. Модели политик безопасности. Политики избирательного разграничения доступа

Исходная политика избирательного разграничения доступа к информации (дискреционная модель) формируется путем задания администратором набора троек следующего вида , где - субъект доступа, - объект доступа, - множество прав доступа, которыми наделен субъект к объекту (например, чтение, запись, исполнение и т.д.) .

При формировании дискреционной политики безопасности обычно формируют дискреционную матрицу доступов , строки которой соответствуют субъектам системы, столбцы – объектам, а в ячейках матрицы хранят множество типов доступов. Пример данной матрицы представлен в таблице

Дискреционная матрица доступов.

Объект / Субъект	**Файл_1**	**Файл_2**	**CD-RW**	**Флоппи-дисковод**
Администратор	Полные права	Полные права	Полные права	Полные права
Гость	Запрет	Чтение	Чтение	Запрет
Пользователь_1	Чтение, передача прав	Чтение, запись	Полные права	Полный запрет

Для матрицы доступа, представленной в таблице, Пользователь_1 имеет права на чтение и запись в Файл_2. Передавать эти права другому пользователю он не может.

Модель безопасности Харрисона-Руззо-Ульмана (HRU) является классической дискреционной моделью реализующей произвольное управление доступом субъектов к объектам и контроль за распространением прав доступа.

16. Идентификация и аутентификация субъектов

Реализация никакой из политик безопасности не будет возможна в случае, если компьютерная система не сможет распознать (идентифицировать) субъекта, пытающегося получить доступ к объекту компьютерной системы. Поэтому минимально защищенная КС должна включать в себя подсистему идентификации, позволяющую идентифицировать инициирующего доступ субъекта.

Под идентификацией понимают присвоение пользователю некоторого уникального идентификатора, который он должен предъявить СЗИ при осуществлении доступа к объекту, то есть назвать себя. Используя предъявленный пользователем идентификатор, СЗИ может проверить наличие данного пользователя в списке зарегистрированных и авторизовать его (то есть наделить полномочиями) для выполнения определенных задач.

В качестве идентификаторов могут использоваться, например, имя пользователя (логин), аппаратные устройства типа iButton (Touch Memory), бесконтактные радиочастотные карты proximity, пластиковые карты и т.д.

Идентификаторы субъектов не являются секретной информацией и могут храниться в КС в открытом виде.

Для нейтрализации угроз, связанных с хищением идентификаторов и подмены злоумышленником легального пользователя необходимы дополнительные проверки субъекта, заключающиеся в подтверждении им владения предъявленным идентификатором. Данные проверки проводятся на этапе аутентификации пользователя.

Под аутентификацией понимают подтверждение пользователем предъявленного идентификатора, проверка его подлинности и принадлежности именно данному пользователю. Аутентификация выполняется для устранения фальсификации на этапе идентификации.

В качестве аутентифицирующей информации может использоваться, например, пароль, секретный код, пин-код и т.д. Информация, используемая субъектом для аутентификации, должна сохраняться им в секрете. Хищение данной информации злоумышленником ведет к тому, что злоумышленник сможет пройти этап идентификации и аутентификации без обнаружения фальсификации.

Этапы идентификации и аутентификации пользователя объединяются в единой подсистеме, называемой подсистемой идентификации и аутентификации (И/АУ).

17. Парольные системы идентификации и аутентификации пользователей. Основные требования к выбору и использованию паролей

Парольные системы идентификации/аутентификации является одними из основных и наиболее распространенных в СЗИ методов пользовательской аутентификации. В данном случае информацией, аутентифицирующей пользователя, является некоторый секретный пароль, известный только легальному пользователю.

Совокупность идентификатора и пароля пользователя называется его учетной записью. База данных пользователей парольной системы содержит учетные записи всех ее пользователей.

Парольные системы являются зачастую «передним краем обороны» всей системы безопасности. Отдельные ее элементы могут быть расположены в местах, открытых для доступа потенциальному злоумышленнику (в том числе и база данных учетных записей пользователей). В связи с этим, парольные системы становятся одним из наиболее привлекательных для злоумышленника объектов атаки. Основными типами угроз безопасности парольных систем являются следующие.

1. Перебор паролей в интерактивном режиме.
2. Подсмотр пароля.
3. Преднамеренная передача пароля его владельцем другому лицу.
4. Кража базы данных учетных записей с дальнейшим ее анализом, подбором пароля.
5. Перехват вводимого пароля путем внедрения в КС программных закладок (клавиатурных шпионов); перехват пароля, передаваемого по сети.
6. Социальная инженерия.

Многие недостатки парольных систем связаны с наличием человеческого фактора, который проявляется в том, что пользователь, зачастую, стремится выбрать пароль, который легко запомнить (а значит и подобрать), записать сложно запоминаемый пароль, ввести пароль так, что его могут увидеть посторонние, передать пароль другому лицу намеренно или под влиянием заблуждения.

18. Парольные системы идентификации и аутентификации пользователей. Количественная оценка стойкости парольных систем

Количественная оценка стойкости парольных систем может быть выполнена с помощью следующего подхода.

Пусть A – мощность алфавита паролей (количество символов, которые могут быть использованы при составлении пароля). Например, если при составлении пароля могут быть использованы только малые английские буквы, то A=26.

L – длина пароля.

$S = A^L$ - число всевозможных паролей длины L, которые можно составить из символов алфавита A.

V – скорость перебора паролей злоумышленником.

T – максимальный срок действия пароля.

Тогда, вероятность P подбора пароля злоумышленником в течении срока его действия T определяется по следующей формуле.

$$P = \frac{V * T}{S} = \frac{V * T}{A^L}$$

Эту формулу можно обратить для решения следующей задачи:

ЗАДАЧА. Определить минимальные мощность алфавита паролей A и длину паролей L, обеспечивающих вероятность подбора пароля злоумышленником не более заданной P, при скорости подбора паролей V, максимальном сроке действия пароля T.

Данная задача имеет неоднозначное решение. При исходных данных V,T,P однозначно можно определить лишь нижнюю границу S* числа всевозможных паролей. Целочисленное значение нижней границы вычисляется по формуле

$$S^* = \left\lceil \frac{V * T}{P} \right\rceil \quad (1)$$

где - целая часть числа, взятая с округлением вверх.

После нахождения нижней границы S* необходимо выбрать такие A и L, чтобы выполнялось неравенство (2).

$$S^* \le S = A^L \quad (2)$$

При выборе S, удовлетворяющего неравенству (2), вероятность подбора пароля злоумышленником (при заданных V и T) будет меньше или равна P.

При вычислениях по формулам (1) и (2), величины должны быть приведены к одной размерности.

19. Идентификация и аутентификация пользователей с использованием технических устройств

При идентификации/аутентификации пользователей с использованием физических устройств, в качестве пользовательского идентификатора используется некоторое техническое устройство, содержащее уникальный идентификационный номер, используемый для решения задач идентификации владельца, а в отдельных случаях и секретную аутентифицирующую информацию, ограничивающую доступ к устройству. Широко распространенными техническими устройствами, используемыми для решения задач идентификации/аутентификации пользователей являются:

- идентификаторы iButton (Touch Memory);
- бесконтактные радиочастотные карты proximity;
- пластиковые карты;
- ключи e-Token.

20. Идентификация и аутентификация с использованием индивидуальных биометрических характеристик пользователя

Под биометрикой понимается использование для аутентификации личности индивидуальных признаков человека. В качестве биометрических характеристик, которые могут быть использованы при аутентификации субъекта доступа, можно указать следующие:

1. отпечатки пальцев;
2. геометрическая форма рук;
3. узор радужной оболочки и сетчатки глаз;
4. форма и размеры лица;
5. особенности голоса;
6. биомеханические характеристики почерка;
7. биомеханические характеристики «клавиатурного почерка».

Особенностью применения биометрических систем идентификации и аутентификации личности по сравнению с другими классами систем И/АУ являются следующие:

1. Необходимость обучения биометрической системы для конкретных пользователей, зачастую, достаточно длительного.
2. Возможность ошибочных отказов и ошибочных подтверждений при аутентификации пользователей.
3. Необходимость использования специальных технических устройств для чтения биометрических характеристик, как правило, достаточно дорогостоящих (за исключением, быть может, аутентификации по клавиатурному почерку).

4.2.2. Практическое задание

4.2.2.1. Порядок проведенияи 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.

26-30 баллов ставится, если обучающимся:

Задание выполнено полностью и правильно.

21-25 баллов ставится, если обучающимся:

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

17-20 баллов ставится, если обучающимся:

Задание выполнено частично или с фактическими и вычислительными ошибками.

0-16 баллов ставится, если обучающимся:

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

4.2.2.3. Оценочные средства.

Задание 1. Зашифруйте слово «защита» шифром Гронсфельда с ключом 12 и алфавитом «абвгдеёжзийклмнопрстуфхцчшщъыьэюя».

Ответ: ивъкув

Задание 2. Зашифруйте слово «экзамен» шифром Цезаря с ключом 5 и используя алфавит «абвгдеёжзийклмнопрстуфхцчшщъыьэюя».

Ответ: впмесйт

Задание 3. Зашифруйте слово «информация» шифром Виженера с ключом "защита" и используя алфавит «абвгдеёжзийклмнопрстуфхцчшщъыьэюя».

Ответ: рннчгмзцвз

Задание 4. Зашифруйте текст «БАГАЖ» шифром Цезаря с ключам К=3.

Ответ: ДГЖГЙ

Задание 5. Зашифровать текст «Дом», используя шифр простой моноалфавитной замены.

Ответ: ЫАЙ

Задание 6. Зашифровать открытый текст «НЕРУКОТВОРНЫЙ» с помощью шифрующей таблицы Трисемуса.

Ответ: ЖУЩЫЙШЕОШЩЖТЦ

Задание 7. Необходимо зашифровать исходное сообщение «НОЧЕВАЛА ТУЧКА ЗОЛОТАЯ» шифром Гронсфельда, в качестве ключа взять К=193431.

Ответ: ОЧЪИЕБМИХЧЪЛБРСПСУБЗ

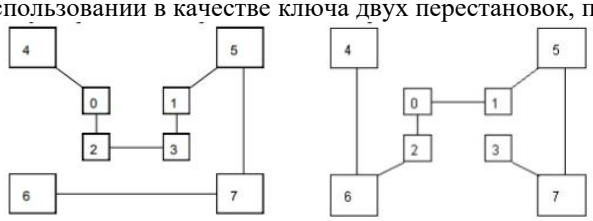
Задание 8. Зашифровать сообщение ПРИЛЕТАЮ ДНЕМ по методу Вижинера с помощью ключевого слова СИСТЕМА

Ответ: БЩЮЙЯАП МЯЧС

Задание 9. Зашифровать открытый текст «ПРИЕЗЖАЮДНЕМ» методом перестановки с ключом К=3142**.**

Ответ: ИПЕР АЗЮЖ ЕДМН

Задание 10. Зашифруйте открытый текст «ВОСЕМЬ МАРШРУТОВ» с помощью перестановок Гамильтона при использовании в качестве ключа двух перестановок, представленных на рис.



Ответ: МВСЕСЬМ УОШАРТВР

Приложение 2
к рабочей программе дисциплины (модуля)
Б1.О.05.07 Информационная безопасность

Перечень литературы, необходимой для освоения дисциплины (модуля)

Направление подготовки: 15.03.06 Мехатроника и робототехника

Профиль подготовки: Физические основы мехатроники и робототехники

Квалификация выпускника: бакалавр

Форма обучения: очная

Язык обучения: русский

Год начала обучения по образовательной программе: 2025

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. 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.

4. 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.

5. 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.О.05.07 Информационная безопасность

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

Направление подготовки: 15.03.06 Мехатроника и робототехника

Профиль подготовки: Физические основы мехатроники и робототехники

Квалификация выпускника: бакалавр

Форма обучения: очная

Язык обучения: русский

Год начала обучения по образовательной программе: 2025

Освоение дисциплины (модуля) предполагает использование следующего программного обеспечения и информационно-справочных систем:

Программное обеспечение: операционнаясистемаWindows, Microsoftoffice, PyCharm, KasperskyFreeдляWindows
Электронная библиотечная система «ZNANIUM.COM»
Электронная библиотечная система Издательства «Лань»
Электронная библиотечная система «Консультант студента»