МИНОБРНАУКИ РОССИИ
Федеральное государственное бюджетное
образовательное учреждение высшего образования
«Астраханский государственный университет имени В. Н. Татищева»
(Астраханский государственный университет им. В. Н. Татищева)

СОГЛАСОВАНО
Руководитель ОПОП
А.В. Григорьев
«23» мая 2023 г.

УТВЕРЖДАЮ
И.о .заведующего кафедрой
информационной безопасности
Р.Ю. Демина
«23» мая 2023 г.

РАБОЧАЯ ПРОГРАММА ДИСЦИПЛИНЫ (МОДУЛЯ)
«Безопасность информационных технологий и систем»

наименование дисциплины (модуля)

Составитель(-и)	**Гурская Т.Г., доцент, к.т.н., доцент кафедры информационной безопасности**
	Мартьянова А.Е., доцент, к.т.н., доцент кафедры информационной безопасности
Направление подготовки	**09.03.03 Прикладная информатика**
Направленность (профиль) ОПОП	**«Прикладная информатика в социальных науках»**
Квалификация (степень)	**бакалавр**
Форма обучения	**очная**
Год приема	**2023**
Курс	**3**
Семестр	**6**

Астрахань, 2023

1. ЦЕЛИ И ЗАДАЧИ ОСВОЕНИЯ ДИСЦИПЛИНЫ (МОДУЛЯ)

1.1. Целью освоения дисциплины (модуля) «Безопасность информационных технологий и систем» является формирование у студентов с позиций системного подхода, теории информации, теории моделирования, искусственного интеллекта и других наук, и прикладных разделов информатики реализуется подход к изучению информационных технологий, как науки о промышленных способах переработки, преобразования и использования информации.

1.2. Задачами освоения дисциплины (модуля) *являются*:

- Рассмотреть понятия, виды и свойства информации.
- Определить основные понятия и задачи информационной технологии, этапы эволюции.
- Раскрыть базовые информационные процессы, входящие в состав информационных технологий.

2. МЕСТО ДИСЦИПЛИНЫ (МОДУЛЯ) В СТРУКТУРЕ ОПОП

2.1. Учебная дисциплина «Безопасность информационных технологий и систем**»** Б1.Б.10.02 входит в обязательную (базовую) часть учебного плана направления подготовки 09.03.03 «Прикладная информатика», профиль «Прикладная информатика в социальных науках» 2023 года набора и относится к обязательной (базовой) части. Дисциплина изучается в 6 семестре, общая трудоемкость дисциплины – 4 ЗЕ, 144 часа, итоговая форма контроля – экзамен.

2.2. Для изучения данной учебной дисциплины (модуля) необходимы следующие знания, умения, навыки, формируемые предшествующими учебными дисциплинами (модулями):

- Введение в информационные технологии.
- Математические основы информационных технологий и вычислительной техники.

В результате освоения этих дисциплин, студент должен иметь:

Знания:

– основных современных информационных технологий и программных средств;

– основных понятий и методов математического анализа;

− основных понятий и методов линейной алгебры и теории алгебраических систем.

Умения:

− использовать программные и аппаратные средства персонального компьютера;

− использовать математические методы и модели для решения прикладных задач.

Навыки:

– владения методами количественного анализа процессов обработки, поиска и передачи информации;

– поиска информации в глобальной информационной сети Интернет и работы с офисными приложениями (текстовыми процессорами, электронными таблицами, средствами подготовки презентационных материалов, СУБД и т. п.);

– владения теоретического и экспериментального исследования объектов профессиональной деятельности.

2.3. Последующие учебные дисциплины (модули) и (или) практики, для которых необходимы знания, умения, навыки, формируемые данной учебной дисциплиной (модулем):

1. Программная инженерия.
2. Производственная практика.
3. Выпускная квалификационная работа.

Знания, полученные в результате изучения дисциплины, используются студентами

при прохождении преддипломной практики и написании бакалаврской работы.

3. ПЛАНИРУЕМЫЕ РЕЗУЛЬТАТЫ ОБУЧЕНИЯ ПО ДИСЦИПЛИНЕ (МОДУЛЮ)

Процесс освоения дисциплины направлен на формирование элементов следующих компетенций в соответствии с ФГОС ВО и ОПОП ВО по данному направлению подготовки (специальности):

а) общепрофессиональных (ОПК):

ОПК-2: Способен понимать принципы работы современных информационных технологий и программных средств, в том числе отечественного производства, и использовать их при решении задач профессиональной деятельности

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

Таблица 1 - Декомпозиция результатов обучения

Код и наименование компетенции	Планируемые результаты обучения по дисциплине (модулю)		
	Знать (1)	Уметь (2)	Владеть (3)
ОПК-2. Способен понимать принципы работы современных информационных технологий и программных средств, в том числе отечественного производства, и использовать их при решении задач профессиональной деятельности	ИОПК-2.1. Знать: современные информационные технологии и программные средства, в том числе отечественного производства, при решении задач профессиональной деятельности.	ИОПК-2.2. Уметь: выбирать современные информационные технологии и программные средства, в том числе отечественного производства, при решении задач профессиональной деятельности	ИОПК-2.3. Иметь навыки: применения современных информационных технологий и программных средств, в том числе отечественного производства, при решении задач профессиональной деятельности
ОПК-3. Способен решать стандартные задачи профессиональной деятельности на основе информационной и библиографической культуры с применением информационно-коммуникационных технологий и с учетом основных требований информационной безопасности.	ИОПК-3.1. Знать: принципы, методы и средства решения стандартных задач профессиональной деятельности на основе информационной и библиографической культуры с применением информационно-коммуникационных технологий и с учетом основных требований информационной	ИОПК-3.2. Уметь: решать стандартные задачи профессиональной деятельности на основе информационной и библиографической культуры с применением информационно-коммуникационных технологий и с учетом основных требований информационной безопасности	ИОПК-3.3. Иметь навыки: подготовки обзоров, аннотаций, составления рефератов, научных докладов, публикаций и библиографии по научно-исследовательской работе с учетом требований информационной безопасности

	безопасности		

4. СТРУКТУРА И СОДЕРЖАНИЕ ДИСЦИПЛИНЫ «Безопасность информационных технологий и систем»

Объем дисциплины (модуля) 4 ЗЕ, 144 часа, 51 час выделен на контактную работу обучающихся с преподавателем (из них 17 часов – лекции, 34 часов – лабораторные работы), 93 часа – на самостоятельную работу обучающихся.

Таблица 2 – Структура и содержание дисциплины (модуля)

№ п/п	Наименование радела (темы)	Семестр	Неделя семестра	Контактная работа (в часах)			Самостоят. работа		Формы текущего контроля успеваемости *(по неделям семестра)* Форма промежуточной аттестации *(по семестрам)*
				Л	ПЗ	ЛР	КР	СР	
1	Введение в дисциплину	4	1-2	2		4		12	Опрос по теме. Лабораторная работа 1
2	Обеспечение ИБ на уровне государства		3-4	2		4		12	Опрос по теме. Лабораторная работа 2
3	Система безопасности		5-6	2		4		12	Опрос по теме. Лабораторная работа 3
4	Основы криптографии		7-8	2		4		12	Опрос по теме. Лабораторная работа 4
5	Электронная подпись		9-10	2		4		12	Опрос по теме. Лабораторная работа 5
6	Компьютерная стеганография		11-12	2		4		12	Опрос по теме. Лабораторная работа 6
7	Построение защищенных экономических систем		13-14	2		4		12	Опрос по теме. Лабораторная работа 7
8	Защищенные компьютерные системы		15-18	3		6		9	Опрос по теме. Лабораторная работа 8. Контрольная работа 1
ИТОГО			**144**	**17**		**34**		**93**	**Экзамен**

Условные обозначения:

Л – занятия лекционного типа; ПЗ – практические занятия, ЛР – лабораторные работы; КР – курсовая работа; СР – самостоятельная работа по отдельным темам

Таблица 3 - Матрица соотнесения тем/разделов учебной дисциплины/модуля и формируемых компетенций

Темы, разделы дисциплины	*Кол-во часов*	*Компетенции*		*Σ общее количество компетенций*
		ОПК-2	ОПК-3	
Введение в дисциплину	18	+	+	2
Обеспечение ИБ на уровне государства	18	+	+	2
Система безопасности	18	+	+	2
Основы криптографии	18	+	+	2
Электронная подпись	18	+	+	2
Компьютерная стеганография	18	+	+	2
Построение защищенных экономических систем	18	+	+	2
Защищенные компьютерные системы	18	+	+	2
ИТОГО	144			

Краткое содержание каждой темы дисциплины (модуля)

Раздел 1. Введение в дисциплину

Цели и задачи информационной безопасности.

Основные положения теории информационной безопасности: информация и информационные отношения; субъекты информационных отношений, их безопасность. Три вида возможных нарушений ИС. Определение требований к защищенности информации. ГОСТ 34.003-90 «Информационная технология. Комплекс стандартов на автоматизированные системы. Термины и определения». ГОСТ 34.201-89 «Информационная технология. Комплекс стандартов на автоматизированные системы. Виды, комплектность и обозначение документов при создании автоматизированных систем». ГОСТ 34.601-90 «Информационная технология. Комплекс стандартов на автоматизированные системы. Автоматизированные системы. Стадии создания». ГОСТ 34.602-89 «Информационная технология. Комплекс стандартов на автоматизированные системы. Техническое задание на создание автоматизированной системы».

Раздел 2. Обеспечение ИБ на уровне государства

Место информационной безопасности в национальной безопасности РФ.

Законодательные и правовые основы защиты компьютерной информации и информационных технологий. Международные стандарты информационного обмена. ИБ в условиях функционирования в России глобальных сетей. Назначение и задачи в сфере обеспечения ИБ на уровне государства. BS 25999 и ГОСТ Р 53647 – управление непрерывностью бизнеса. СТО БР ИББС-1.0 – общие положения в области обеспечения ИБ организаций банковской системы Российской Федерации. СТО БР ИББС-1.1 – аудит ИБ 78. СТО БР ИББС-1.2 – методика оценки соответствия ИБ организаций банковской системы Российской Федерации требованиям СТО БР ИББС-1.0. Рекомендации по стандартизации Р 50.1.053-2005. Информационные технологии. Основные термины и определения в области технической защиты информации. (утв. Приказом Ростехрегулирования от 06.04.2005 № 77-ст). Рекомендации по стандартизации Р 50.1.056-2005. Техническая защита информации. Основные термины и определения. (утв. Приказом Ростехрегулирования от 29.12.2005 № 479-ст).

Раздел 3. Система безопасности

Построение системы защиты информации в организации. Современные методики анализа и управления рисками информационной безопасности. Основные программно-технические

меры безопасности информации: идентификация и аутентификация; управление доступом. Основные программно-технические меры безопасности информации: протоколирование, аудит, шифрование, контроль целостности, электронная подпись.
Проблемы защиты информации в информационных системах. Задачи системы безопасности. Меры противодействия угрозам безопасности. Классификация мер. Основные нормативные руководящие документы, касающиеся государственной тайны, нормативно-справочные документы. Основные механизмы защиты АС. Модели безопасности и их применение. ISO/IEC 27001:2005 и ГОСТ Р ИСО/МЭК 27001–2006 – требования к СУИБ. ISO/IEC 27002:2005 и ГОСТ Р ИСО/МЭК 17799–2005 – практические правила управления ИБ. ISO/IEC 27003:2010 – руководство по внедрению СУИБ. ISO/IEC 27004:2009 и ГОСТ Р ИСО/МЭК 27004–2011 – оценка функционирования СУИБ.

Раздел 4. Основы криптографии

Современные криптосистемы для защиты компьютерной информации. Способы симметрического шифрования. Современные алгоритмы симметрического шифрования. Основные понятия и классификация средств криптографической защиты информации. Абсолютно стойкий шифр. Принципы создания и свойства асимметрических криптосистем. Примеры асимметрических криптосистем. Методы криптографии. Классификация шифров по различным признакам.

Раздел 5. Электронная подпись

Электронная цифровая подпись и ее использование. Основные понятия и свойства. Аппаратно-программные средства защиты информации. Средства обеспечения конфиденциальности данных; средства идентификации и аутентификации пользователей.

Раздел 6. Компьютерная стеганография

Компьютерная стеганография и ее применение. Базовые понятия стеганографии Модель стеганографической системы. Понятие контейнера, виды контейнеров. Методы сокрытия информации в мультимедийных файлах. Направления развития компьютерной стеганографии.

Раздел 7. Построение защищенных экономических систем

Основные технологии построения защищенных систем.
Для каждого из рассматриваемых процессов, таких как извлечение информации, транспортирование, обработка, хранение, представление и использование информации, дается подробная характеристика с раскрытием моделей и современного состояния. Детально раскрываются базовые информационные технологии, к которым отнесены: мультимедиа технологии, геоинформационные, технологии защиты информации, CASE-технологии, телекоммуникационные технологии, технологии искусственного интеллекта, технологии программирования, облачные технологии, технология больших данных. Приводится анализ прикладных информационных технологий для различных предметных областей, в частности, технологий корпоративного управления. Дается анализ и приводятся рекомендации по использованию программных, технических и методических средств информационных технологий. Излагается технология построения информационных систем, что особо актуально для формирования профессионалов-разработчиков. Приводятся основы системного подхода применительно к задачам построения информационных систем.
Методы идентификации и проверки подлинности пользователей информационных систем. Основные технологии построения защищенных ЭИС. Место ИБ экономических систем в национальной безопасности страны. Концепция ИБ. Особенности работы с персоналом, владеющим конфиденциальной информацией. Технологические основы обработки конфиденциальных документов. ISO/IEC 27005:2011 и ГОСТ Р ИСО/МЭК 27005–2010 – управление рисками ИБ. ISO/IEC 27006:2011 и ГОСТ Р ИСО/МЭК 27006–2008 – требования к органам, осуществляющим аудит и сертификацию СУИБ. ISO/IEC 27007:2011 и ISO/IEC 27008:2011 – руководства по аудиту СУИБ и средств управления ИБ,

реализованных в СУИБ. ISO/IEC 27011:2008 – руководство по управлению ИБ для телекоммуникационных компаний на основе ISO/IEC 27002.

Раздел 8. Защищенные компьютерные системы

Использование защищенных компьютерных систем. Защита операционной системы и других системных программных средств. Организация доступа в локальных сетях. ISO/IEC 27013 – руководство по интегрированному внедрению стандартов ISO/IEC 20000 и 27001. ISO/IEC 27014 – инфраструктура руководства ИБ. ISO/IEC 27015 – руководство по управлению ИБ для финансовых сервисов. ISO/IEC 27031:2011 – руководство по готовности информационных и телекоммуникационных технологий для обеспечения непрерывности бизнеса.

5. МЕТОДИЧЕСКИЕ УКАЗАНИЯ ПО ПРЕПОДАВАНИЮ И ОСВОЕНИЮ ДИСЦИПЛИНЫ (МОДУЛЯ)

5.1. Указания для преподавателей по организации и проведению учебных занятий по дисциплине (модулю)

При подготовке к лекционным занятиям необходимо воспользоваться учебно-методической литературой из п.8 (основной). Лекции необходимо проводить с использованием презентаций, созданных в Microsoft PowerPont.

При подготовке к лабораторным занятиям необходимо воспользоваться учебно-методической литературой из п.8 (дополнительной).

5.2. Указания для обучающихся по освоению дисциплины (модулю)

Во время самостоятельной работы необходимо воспользоваться учебно-методической литературой из п.8 (основной), (дополнительной), Интернет-источниками.

Таблица 4 – Содержание самостоятельной работы обучающихся

Номер радела (темы)	*Темы/вопросы, выносимые на самостоятельное изучение*	*Кол-во часов*	*Формы работы*
1.	Опрос по теме. Лабораторная работа 1.	12	Внеаудиторная, изучение учебных пособий
2.	Опрос по теме. Лабораторная работа 2.	12	Внеаудиторная, изучение учебных пособий
3.	Опрос по теме. Лабораторная работа 3.	12	Внеаудиторная, изучение учебных пособий
4.	Опрос по теме. Лабораторная работа 4.	12	Внеаудиторная, изучение учебных пособий
5.	Опрос по теме. Лабораторная работа 5.	12	Внеаудиторная, изучение учебных пособий
6.	Опрос по теме. Лабораторная работа 6.	12	Внеаудиторная, изучение учебных пособий
7.	Опрос по теме. Лабораторная работа 7.	12	Внеаудиторная, изучение учебных

			пособий
8.	Опрос по теме. Лабораторная работа 8. Контрольная работа 1.	9	Внеаудиторная, изучение учебных пособий

5.3. Виды и формы письменных работ, предусмотренных при освоении дисциплины (модуля), выполняемые обучающимися самостоятельно

Не предусмотрено.

6. ОБРАЗОВАТЕЛЬНЫЕ И ИНФОРМАЦИОННЫЕ ТЕХНОЛОГИИ

При реализации различных видов учебной работы по дисциплине могут использоваться электронное обучение и дистанционные образовательные технологии.

6.1. Образовательные технологии

Таблица 5 – Образовательные технологии, используемые при реализации учебных занятий

Раздел, тема дисциплины (модуля)	Форма учебного занятия		
	Лекция	Практическое занятие, семинар	Лабораторная работа
Введение в дисциплину	Обзорная лекция	Не предусмотрено	выполнение лабораторной работы
Обеспечение ИБ на уровне государства	Лекция - презентация	Не предусмотрено	выполнение лабораторной работы
Система безопасности	Лекция - презентация	Не предусмотрено	выполнение лабораторной работы
Основы криптографии	Обзорная лекция	Не предусмотрено	выполнение лабораторной работы
Электронная подпись	Лекция - презентация	Не предусмотрено	выполнение лабораторной работы
Компьютерная стеганография	Лекция - презентация	Не предусмотрено	выполнение лабораторной работы
Построение защищенных экономических систем	Лекция - презентация	Не предусмотрено	выполнение лабораторной работы
Защищенные компьютерные системы	Обзорная лекция	Не предусмотрено	выполнение лабораторной работы

Учебные занятия по дисциплине могут проводиться с применением информационно-телекоммуникационных сетей при опосредованном (на расстоянии) интерактивном взаимодействии обучающихся и преподавателя в режимах on-line в формах: видеолекций, лекций-презентаций, видеоконференции, собеседования в режиме чат, форума, чата, выполнения виртуальных практических и/или лабораторных работ и др.

Максимальный объем занятий обучающегося с применением электронных

образовательных технологий не должен превышать 25%.

6.2. Информационные технологии

– использование возможностей интернета в учебном процессе (использование сайта преподавателя (рассылка заданий, предоставление выполненных работ, ответы на вопросы, ознакомление обучающихся с оценками и т. д.));

– использование электронных учебников и различных сайтов (например, электронных библиотек, журналов и т. д.) как источников информации;

– использование возможностей электронной почты преподавателя;

– использование средств представления учебной информации (электронных учебных пособий и практикумов, применение новых технологий для проведения очных (традиционных) лекций и семинаров с использованием презентаций и т. д.);

– использование интегрированных образовательных сред, где главной составляющей являются не только применяемые технологии, но и содержательная часть, т. е. информационные ресурсы (доступ к мировым информационным ресурсам, на базе которых строится учебный процесс);

– использование виртуальной обучающей среды (LMS Moodle «Цифровое обучение») или иных информационных систем, сервисов и мессенджеров]

6.3. Программное обеспечение, современные профессиональные базы данных и информационные справочные системы

6.3.1. Программное обеспечение

Наименование программного обеспечения	Назначение
Adobe Reader	Программа для просмотра электронных документов
Платформа дистанционного обучения LMS Moodle	Виртуальная обучающая среда
Mozilla FireFox	Браузер
Microsoft Office 2013, Microsoft Office Project 2013 , Microsoft Office Visio 2013	Офисная программа
7-zip	Архиватор
Microsoft Windows 7 Professional	Операционная система
Kaspersky Endpoint Security	Средство антивирусной защиты

6.3.2. Современные профессиональные базы данных и информационные

справочные системы

a) Электронный каталог Научной библиотеки АГУ на базе MARK SQL НПО «Информ-систем»: https://library.asu.edu.ru.
b) Электронный каталог «Научные журналы АГУ»: http://journal.asu.edu.ru/.
c) Универсальная справочно-информационная полнотекстовая база данных периодических изданий ООО «ИВИС»: http://dlib.eastview.com/
d) Электронно-библиотечная система elibrary. http://elibrary.ru
e) Справочная правовая система КонсультантПлюс: http://www.consultant.ru
f) Информационно-правовое обеспечение «Система ГАРАНТ»: http://garant-astrakhan.ru

7. ФОНД ОЦЕНОЧНЫХ СРЕДСТВ ДЛЯ ПРОВЕДЕНИЯ ТЕКУЩЕГО КОНТРОЛЯ И ПРОМЕЖУТОЧНОЙ АТТЕСТАЦИИ ПО ДИСЦИПЛИНЕ (МОДУЛЮ)

7.1. Паспорт фонда оценочных средств

При проведении текущего контроля и промежуточной аттестации по дисциплине (модулю) «Безопасность информационных технологий и систем» проверяется сформированность у обучающихся компетенций, указанных в разделе 3 настоящей программы. Этапность формирования данных компетенций в процессе освоения образовательной программы определяется последовательным освоением дисциплин (модулей) и прохождением практик, а в процессе освоения дисциплины (модуля) – последовательным достижением результатов освоения содержательно связанных между собой разделов, тем.

Таблица 6 – Соответствие изучаемых разделов, результатов обучения и оценочных средств

№ п/п	Контролируемые разделы (темы) дисциплины*	Код контролируемой компетенции (или ее части)	Наименование оценочного средства
1.	Введение в дисциплину	ОПК-2, ОПК-3	Вопросы для обсуждения. Лабораторная работа 1
2.	Обеспечение ИБ на уровне государства	ОПК-2, ОПК-3	Вопросы для обсуждения. Лабораторная работа 2
3.	Система безопасности	ОПК-2, ОПК-3	Вопросы для обсуждения. Лабораторная работа 3
4.	Основы криптографии	ОПК-2, ОПК-3	Вопросы для обсуждения. Лабораторная работа 4
5.	Электронная подпись	ОПК-2, ОПК-3	Вопросы для обсуждения. Лабораторная работа 5
6.	Компьютерная стеганография	ОПК-2, ОПК-3	Вопросы для обсуждения. Лабораторная работа 6
7.	Построение защищенных экономических систем	ОПК-2, ОПК-3	Вопросы для обсуждения.

			Лабораторная работа 7
8.	Защищенные компьютерные системы	ОПК-2, ОПК-3	Вопросы для обсуждения. Лабораторная работа 8. Контрольная работа 1

7.2. Описание показателей и критериев оценивания компетенций, описание шкал оценивания

Таблица 7 – Показатели оценивания результатов обучения в виде знаний

Шкала оценивания	Критерии оценивания
5 «отлично»	демонстрирует глубокое знание теоретического материала, умение обоснованно излагать свои мысли по обсуждаемым вопросам, способность полно, правильно и аргументированно отвечать на вопросы, приводить примеры
4 «хорошо»	демонстрирует знание теоретического материала, его последовательное изложение, способность приводить примеры, допускает единичные ошибки, исправляемые после замечания преподавателя
3 «удовлетворительно»	демонстрирует неполное, фрагментарное знание теоретического материала, требующее наводящих вопросов преподавателя, допускает существенные ошибки в его изложении, затрудняется в приведении примеров и формулировке выводов
2 «неудовлетворительно»	демонстрирует существенные пробелы в знании теоретического материала, не способен его изложить и ответить на наводящие вопросы преподавателя, не может привести примеры

Таблица 8 – Показатели оценивания результатов обучения в виде умений и владений

Шкала оценивания	Критерии оценивания
5 «отлично»	демонстрирует способность применять знание теоретического материала при выполнении заданий, последовательно и правильно выполняет задания, умеет обоснованно излагать свои мысли и делать необходимые выводы
4 «хорошо»	демонстрирует способность применять знание теоретического материала при выполнении заданий, последовательно и правильно выполняет задания, умеет обоснованно излагать свои мысли и делать необходимые выводы, допускает единичные ошибки, исправляемые после замечания преподавателя
3 «удовлетворительно»	демонстрирует отдельные, несистематизированные навыки, не способен применить знание теоретического материала при выполнении заданий, испытывает затруднения и допускает ошибки при выполнении заданий, выполняет задание при подсказке преподавателя, затрудняется в формулировке выводов
2 «неудовлетворительно»	не способен правильно выполнить задание

7.3. Контрольные задания или иные материалы, необходимые для результатов обучения по дисциплине (модулю)

Раздел 1. Введение в дисциплину

1. Опрос по теме

Цели и задачи информационной безопасности.
Основные положения теории информационной безопасности: информация и информационные отношения; субъекты информационных отношений, их безопасность. Три вида возможных нарушений ИС. Определение требований к защищенности информации. ГОСТ 34.003-90 «Информационная технология. Комплекс стандартов на автоматизированные системы. Термины и определения». ГОСТ 34.201-89 «Информационная технология. Комплекс стандартов на автоматизированные системы. Виды, комплектность и обозначение документов при создании автоматизированных систем». ГОСТ 34.601-90 «Информационная технология. Комплекс стандартов на автоматизированные системы. Автоматизированные системы. Стадии создания». ГОСТ 34.602-89 «Информационная технология. Комплекс стандартов на автоматизированные системы. Техническое задание на создание автоматизированной системы».

2. Лабораторная работа 1

Парольная защита

Под **несанкционированным доступом к информации** (НСД) согласно руководящим документам Гостехкомиссии будем понимать доступ к информации, нарушающий установленные правила разграничения доступа и осуществляемый с использованием штатных средств, предоставляемых СВТ или АС. НСД может носить случайный или намеренный характер.

Можно выделить несколько обобщенных категорий методов защиты от НСД, в частности:

1. организационные;
2. технологические;
3. правовые.

К первой категории относятся меры и мероприятия, регламентируемые внутренними инструкциями организации, эксплуатирующей информационную систему. Пример такой защиты — присвоение грифов секретности документам и материалам, хранящимся в отдельном помещении, и контроль доступа к ним сотрудников. Вторую категорию составляют механизмы защиты, реализуемые на базе программно-аппаратных средств, например систем идентификации и аутентификации или охранной сигнализации. Последняя категория включает меры контроля за исполнением нормативных актов общегосударственного значения, механизмы разработки и совершенствования нормативной базы, регулирующей вопросы защиты информации. Реализуемые на практике методы, как правило, сочетают в себе элементы нескольких из перечисленных категорий. Так, управление доступом в помещения может представлять собой взаимосвязь организационных (выдача допусков и ключей) и технологических (установку замков и систем сигнализации) способов защиты.

Рассмотрим подробнее такие взаимосвязанные методы защиты от НСД, как идентификация, аутентификация и используемое при их реализации криптографическое преобразование информации.

Идентификация — это присвоение пользователям идентификаторов и проверка предъявляемых идентификаторов по списку присвоенных.

Аутентификация — это проверка принадлежности пользователю предъявленного им идентификатора. Часто аутентификацию также называют подтверждением или проверкой подлинности.

Под безопасностью (стойкостью) системы идентификации и аутентификации будем понимать степень обеспечиваемых ею гарантий того, что злоумышленник не способен пройти аутентификацию от имени другого пользователя, В этом смысле, чем выше стойкость системы аутентификации, тем сложнее злоумышленнику решить указанную задачу. Система идентификации и аутентификации является одним из ключевых элементов инфраструктуры защиты от НСД любой информационной системы.

Различают три группы методов аутентификации, основанных на наличии у каждого пользователя:

1. индивидуального объекта заданного типа;
2. знаний некоторой известной только ему и проверяющей стороне информации;
3. индивидуальных биометрических характеристик.

К первой группе относятся методы аутентификации, использующие удостоверения, пропуска, магнитные карты и другие носимые устройства, которые широко применяются для контроля доступа в помещения, а также входят в состав программно-аппаратных комплексов защиты от НСД к средствам вычислительной техники.
Во вторую группу входят методы аутентификации, использующие пароли. По экономическим причинам они включаются в качестве базовых средств защиты во многие программно-аппаратные комплексы защиты информации. Все современные операционные системы и многие приложения имеют встроенные механизмы парольной защиты.

Последнюю группу составляют методы аутентификации, основанные на применении оборудования для измерения и сравнения с эталоном заданных индивидуальных характеристик пользователя: тембра голоса, отпечатков пальцев, структуры радужной оболочки глаза и др. Такие средства позволяют с высокой точностью аутентифицировать обладателя конкретного биометрического признака, причем "подделать" биометрические параметры практически невозможно. Однако широкое распространение подобных технологий сдерживается высокой стоимостью необходимого оборудования.

Если в процедуре аутентификации участвуют только две стороны, устанавливающие подлинность друг друга, такая процедура называется непосредственной аутентификацией (direct password authentication). Если же в процессе аутентификации участвуют не только эти стороны, но и другие, вспомогательные, говорят об аутентификации с участием доверенной стороны (trusted third party authentication). При этом третью сторону называют сервером аутентификации (authentication server) или арбитром (arbitrator).

Наиболее распространенные методы аутентификации основаны на применении многоразовых или одноразовых паролей. Из-за своего широкого распространения и простоты реализации парольные схемы часто в первую очередь становятся мишенью атак злоумышленников. Эти методы включают следующие разновидности способов аутентификации:

1. по хранимой копии пароля или его свёртке (plaintext-equivalent);
2. по некоторому проверочному значению (verifier-based);
3. без непосредственной передачи информации о пароле проверяющей стороне (zero-knowledge);
4. с использованием пароля для получения криптографического ключа (cryptographic).

Первую разновидность способов входят системы аутентификации, предполагающие наличие у обеих сторон копии пароля или его свертки. Для организации таких систем требуется создать и поддерживать базу данных, содержащую пароли или сверки паролей всех пользователей. Их слабой стороной является то, что получение злоумышленником

этой базы данных позволяет ему проходить аутентификацию от имени любого пользователя.

Способы, составляющие вторую разновидность, обеспечивают более высокую степень безопасности парольной системы, так как проверочные значения, хотя они и зависят от паролей, не могут быть непосредственно использованы злоумышленником для аутентификации.

Наконец, аутентификация без предоставления проверяющей стороне какой бы то ни было информации о пароле обеспечивает наибольшую степень защиты. Этот способ гарантирует безопасность даже в том случае, если нарушена работа проверяющей стороны (например, в программу регистрации в системе внедрен "троянский конь").

Особым подходом в технологии проверки подлинности являются криптографические протоколы аутентификации. Такие протоколы описывают последовательность действий, которую должны совершить стороны для взаимной аутентификации, кроме того, эти действия, как правило, сочетаются с генерацией и распределением криптографических ключей для шифрования последующего информационного обмена. Корректность протоколов аутентификации вытекает из свойств задействованных в них математических и криптографических преобразований и может быть строго доказана.
Обычные парольные системы проще и дешевле для реализации, но менее безопасны, чем системы с криптографическими протоколами. Последние обеспечивают более надежную защиту и дополнительно решают задачу распределения ключей. Однако используемые в них технологии могут быть объектом законодательных ограничений.

Для более детального рассмотрения принципов построения парольных систем сформулируем несколько основных определений.

Идентификатор пользователя — некоторое уникальное количество информации, позволяющее различать индивидуальных пользователей парольной системы (проводить их идентификацию). Часто идентификатор также называют именем пользователя или именем учетной записи пользователя.

Пароль пользователя — некоторое секретное количество информации, известное только пользователю и парольной системе, которое может быть запомнено пользователем и предъявлено для прохождения процедуры аутентификации. Одноразовый пароль дает возможность пользователю однократно пройти аутентификацию. Многоразовый пароль может быть использован для проверки подлинности повторно.

Учетная запись пользователя — совокупность его идентификатора и его пароля. База данных пользователей парольной системы содержит учетные записи всех пользователей данной парольной системы.

Под **парольной системой** будем понимать программно-аппаратный комплекс, реализующий системы идентификации и аутентификации пользователей АС на основе одноразовых или многоразовых паролей. Как правило, такой комплекс функционирует совместно с подсистемами разграничения доступа и регистрации событий. В отдельных случаях парольная система может выполнять ряд дополнительных функций, в частности генерацию и распределение кратковременных (сеансовых) криптографических ключей.

Основными компонентами парольной системы являются:
- интерфейс пользователя;
- интерфейс администратора;

- модуль сопряжения с другими подсистемами безопасности;
- база данных учетных записей.

Парольная система представляет собой "передний край обороны" всей системы безопасности. Некоторые ее элементы (в частности, реализующие интерфейс пользователя) могут быть расположены в местах, открытых для доступа потенциальному злоумышленнику. Поэтому парольная система становится одним из первых объектов атаки при вторжении злоумышленника в защищенную систему. Ниже перечислены типы угроз безопасности парольных систем:

a Разглашение параметров учетной записи через:
1) подбор в интерактивном режиме;
2) подсматривание;
3) преднамеренную передачу пароля его владельцем другому лицу;
4) захват базы данных парольной системы (если пароли не хранятся в базе в открытом виде, для их восстановления может потребоваться подбор или дешифрование);
5) перехват переданной по сети информации о пароле;
6) хранение пароля в доступном месте.

b Вмешательство в функционирование компонентов парольной системы через:
1) внедрение программных закладок;
2) обнаружение и использование ошибок, допущенных на стадии разработки;
3) выведение из строя парольной системы.

Некоторые из перечисленных типов угроз связаны с наличием так называемого человеческого фактора, проявляющегося в том, что пользователь может:
- выбрать пароль, который легко запомнить и также легко подобрать;
- записать пароль, который сложно запомнить, и положить запись в доступном месте;
- ввести пароль так, что его смогут увидеть посторонние;
- передать пароль другому лицу намеренно или под влиянием заблуждения.

В дополнение к выше сказанному необходимо отметить существование "парадокса человеческого фактора". Заключается он в том, что пользователь нередко стремится выступать скорее противником парольной системы, как, впрочем, и любой системы безопасности, функционирование которой влияет на его рабочие условия, нежели союзником системы защиты, тем самым ослабляя ее. Защита от указанных угроз основывается на ряде перечисленных ниже организационно-технических мер и мероприятий.

Выбор паролей

В большинстве систем пользователи имеют возможность самостоятельно выбирать пароли или получают их от системных администраторов. При этом для уменьшения деструктивного влияния описанного выше человеческого фактора необходимо реализовать ряд требований к выбору и использованию паролей.

Таблица 1

Требование к выбору пароля	**Получаемый эффект**
Установление минимальной длины пароля	Усложняет задачу злоумышленника при попытке подсмотреть пароль или подобрать пароль методом «тотального опробования»
Использование в пароле различных групп символов	Усложняет задачу злоумышленника при попытке подобрать пароль методом «тотального опробования»

Проверка и отбраковка пароля по словарю	Усложняет задачу злоумышленника при попытке подобрать пароль по словарю
Установление максимального срока действия пароля	Усложняет задачу злоумышленника при попытке подобрать пароль методом «тотального опробования», в том числе без непосредственного обращения к системе защиты (режим off-line)
Установление минимального срока действия пароля	Препятствует попыткам пользователя заменить пароль на старый после его смены по предыдущему требованию
Ведение журнала истории паролей	Обеспечивает дополнительную степень защиты по предыдущему требованию
Применение эвристического алгоритма, бракующего пароли на основании данных журнала истории	Усложняет задачу злоумышленника при попытке подобрать пароль по словарю или с использованием эвристического алгоритма
Ограничение числа попыток ввода пароля	Препятствует интерактивному подбору паролей злоумышленником
Поддержка режима принудительной смены пароля пользователя	Обеспечивает эффективность требования, ограничивающего максимальный срок действия пароля
Использование задержки при вводе неправильного пароля	Препятствует интерактивному подбору паролей злоумышленником
Запрет на выбор пароля самими пользователями и автоматическая генерация паролей	Исключает возможность подобрать пароль по словарю. Если алгоритм генерации паролей не известен злоумышленнику, последний может подбирать пароли только методом «тотального опробования»
Принудительная смена пароля при первой регистрации пользователя в системе	Защищает от неправомерных действия системного администратора, имеющего доступ к паролю в момент создания учетной записи

Примеры

Пример 1.
Задание определить время перебора всех паролей, состоящих из 6 цифр.

Алфавит составляют цифры n=10.
Длина пароля 6 символов k=6.

Таким образом, получаем количество вариантов: $C=n^k=10^6$

Примем скорость перебора s=10 паролей в секунду. Получаем время перебора всех паролей t= C/s=10^5секунд□1667минут□28часов□1,2 дня.
Примем, что после каждого из m=3 неправильно введенных паролей идет пауза в v=5 секунд. Получаем время перебора всех паролей
T=t*5/3=16667секунд□2778минут□46часов□1,9 дня.

$T_{итог}$ = t+T = 1,2 + 1,9 = 3,1 дня

Пример 2.
Определить минимальную длину пароля, алфавит которого состоит из 10 символов, время

перебора которого было не меньше 10 лет.
Алфавит составляют символы n=10.

Длина пароля рассчитывается: $k=\log_n C= \lg C$.

Определим количество вариантов C= t * s=10лет*10 паролей в сек. =
10*10*365*24*60*60 3,15* 10^9 вариантов

Таким образом, получаем длину пароля: $k=\lg (3,15*10^9) = 9,5$ Очевидно, что длина пароля должна быть не менее 10 символов.

Задания

- Определить время перебора всех паролей с параметрами. Алфавит состоит из n символов.

Длина пароля символов k.
Скорость перебора s паролей в секунду.
После каждого из m неправильно введенных паролей идет пауза в v секунд

вариант	n	k	s	m	v
1	33	10	100	0	0
2	26	12	13	3	2
3	52	6	30	5	10
4	66	7	20	10	3
5	59	5	200	0	0
6	118	9	50	7	12
7	128	10	500	0	0
8	150	3	200	5	3
9	250	8	600	7	3
10	500	5	1000	10	10

- Определить минимальную длину пароля, алфавит которого состоит из n символов, время перебора которого было не меньше t лет.

Скорость перебора s паролей в секунду.

вариант	n	t	s
1	33	100	100
2	26	120	13
3	52	60	30
4	66	70	20
5	59	50	200
6	118	90	50
7	128	100	500
8	150	30	200
9	250	80	600
10	500	50	1000

- Определить количество символов алфавита, пароль состоит из k символов, время перебора которого было не меньше t лет.

Скорость перебора s паролей в секунду.

вариант	k	t	s
1	5	100	100
2	6	120	13
3	10	60	30
4	7	70	20
5	9	50	200
6	11	90	50
7	12	100	500
8	6	30	200
9	8	80	600
10	50	50	1000

Раздел 2. Обеспечение ИБ на уровне государства

1. Опрос по теме

Место информационной безопасности в национальной безопасности РФ.
Законодательные и правовые основы защиты компьютерной информации и информационных технологий. Международные стандарты информационного обмена. ИБ в условиях функционирования в России глобальных сетей. Назначение и задачи в сфере обеспечения ИБ на уровне государства. BS 25999 и ГОСТ Р 53647 – управление непрерывностью бизнеса. СТО БР ИББС-1.0 – общие положения в области обеспечения ИБ организаций банковской системы Российской Федерации. СТО БР ИББС-1.1 – аудит ИБ 78. СТО БР ИББС-1.2 – методика оценки соответствия ИБ организаций банковской системы Российской Федерации требованиям СТО БР ИББС-1.0. Рекомендации по стандартизации Р 50.1.053-2005. Информационные технологии. Основные термины и определения в области технической защиты информации. (утв. Приказом Ростехрегулирования от 06.04.2005 № 77-ст). Рекомендации по стандартизации Р 50.1.056-2005. Техническая защита информации. Основные термины и определения. (утв. Приказом Ростехрегулирования от 29.12.2005 № 479-ст).

2. Лабораторная работа 2

Реализация генератора паролей

1. Теория

Стойкость к взлому подсистемы парольной идентификации (аутентификации) во многом определяется тем, насколько правильно были сформированы пароли пользователей. При несоблюдении ряда требований к выбору паролей, данная стойкость в значительной степени уменьшается, и подсистема идентификации (аутентификации) становится достаточно уязвима при правильно построенной атаке.

Основные требования, которые должны быть учтены при выборе пароля пользователя.

1. Минимальная длина пароля должна быть не менее 6 символов. Сокращение длины пароля во многом повышает вероятность успешной атаки полным их перебором.

2. Пароль должен состоять из различных групп символов (малые и большие латинские буквы, цифры, специальные символы). Использование одной конкретной

группы символов при формировании пароля в значительной степени повышает вероятность атаки по маске.

3. В качестве пароля не должны использоваться реальные слова, имена, фамилии и т. д. Использование в качестве паролей конкретных слов, имен в значительной степени повышает вероятность успешной атаки по словарю.

Иногда генераторы паролей могут использовать при данном генерировании элементы, входящие в идентификатор пользователя (отдельные его символы, количество символов и т. д.). В отдельных вариантах пароль может формироваться даже целиком из идентификатора на основе некоторого алгоритма. В последнем случае заданному идентификатору пользователя ставится в соответствие единственный пароль, который формируется на основе идентификатора.

2. Практика

1. Ознакомиться с теоретической частью работы.
2. Написать программу-генератор паролей.
3. Составить отчет и защитить работу.

Раздел 3. Система безопасности

1. Опрос по теме

Построение системы защиты информации в организации. Современные методики анализа и управления рисками информационной безопасности. Основные программно-технические меры безопасности информации: идентификация и аутентификация; управление доступом. Основные программно-технические меры безопасности информации: протоколирование, аудит, шифрование, контроль целостности, электронная подпись.
Проблемы защиты информации в информационных системах. Задачи системы безопасности. Меры противодействия угрозам безопасности. Классификация мер. Основные нормативные руководящие документы, касающиеся государственной тайны, нормативно-справочные документы. Основные механизмы защиты АС. Модели безопасности и их применение. ISO/IEC 27001:2005 и ГОСТ Р ИСО/МЭК 27001–2006 – требования к СУИБ. ISO/IEC 27002:2005 и ГОСТ Р ИСО/МЭК 17799–2005 – практические правила управления ИБ. ISO/IEC 27003:2010 – руководство по внедрению СУИБ. ISO/IEC 27004:2009 и ГОСТ Р ИСО/МЭК 27004–2011 – оценка функционирования СУИБ.

2. Лабораторная работа 3

Реализация методов парольной защиты

1. Теория

Необходимо изучить технологии аутентификации пользователя на основе пароля.
Аутентификация — процедура проверки подлинности заявленного пользователя, процесса или устройства.
Аутентификацию не следует путать с авторизацией (процедурой предоставления субъекту определенных прав) и идентификацией (процедурой распознавания субъекта по его идентификатору).
Авторизация — процедура предоставления субъекту определенных полномочий и ресурсов в данной системе. Иными словами, авторизация устанавливает сферу действия субъекта и доступные ему ресурсы. Если система не может надежно отличить авторизованное лицо от неавторизованного, конфиденциальность и целостность информации в ней могут быть нарушены. Организации необходимо четко определить свои требования к безопасности, чтобы принимать решения о соответствующих границах авторизации.

С процедурами аутентификации и авторизации тесно связана процедура администрирования действий пользователя.

2. Практика

1. Ознакомиться с теоретической частью работы.
2. Написать программу, представляющую собой форму доступа к определенным информационным ресурсам на основе пароля.
3. Составить отчет и защитить работу.

Раздел 4. Основы криптографии

1. Опрос по теме

Современные криптосистемы для защиты компьютерной информации. Способы симметрического шифрования. Современные алгоритмы симметрического шифрования. Основные понятия и классификация средств криптографической защиты информации. Абсолютно стойкий шифр. Принципы создания и свойства асимметрических криптосистем. Примеры асимметрических криптосистем. Методы криптографии. Классификация шифров по различным признакам.

2. Лабораторная работа 4

Алгоритмы симметричного шифрования.
Шифр простой замены. Таблица Вижинера

1. Теория

Современные криптографические системы тесно связаны с методами шифрования сообщений, которые, в свою очередь, зависят от способа использования ключей. Предлагаемая программа отличается простотой понимания смысла шифрования, позволяет получить криптограммы одного и того же исходного текста в зависимости от выбранного ключевого слова. Кроме того, такой подход шифрования может быть применен в одноключевых криптосистемах для защиты информации в локальных сетях.

Одноключевые криптографические системы являются классическими системами криптографической защиты информации. Для шифрования и расшифрования сообщений в них используется один и тот же ключ, сохранение которого в тайне обеспечивает надежность защиты информации. Шифровальную схему в этом случае можно представить следующим образом:

$$Y = E_Z(X) = D_Z(Y) = D_Z(E_Z(X)),$$

где X — открытый текст;
Y — шифротекст;
D_Z — функция шифрования с секретным ключом z;
E_Z — функция расшифрования с секретным ключом z.

Открытый текст, как правило, имеет произвольную длину. В связи с этим он разбивается на блоки фиксированной длины и каждый блок шифруется в отдельности, независимо от его получения во входной последовательности. Соответствующие методы шифрования называются блочными, а наиболее важными шифрами при этом являются шифры замены (подстановки). Шифры замены образуются с помощью замены знаков исходного сообщения на другие знаки.

Простейшим шифром замены является шифр Цезаря. В этом шифре буквы исходного сообщения латинского алфавита заменяются буквами, расположенными тремя позициями правее. Однако вскрытие таких шифров легко осуществляется путем перебора

всех возможных ключей, в качестве которых используется величина сдвига букв сообщения в алфавите, до появления осмысленного текста.

Устойчивость шифра замены можно повысить за счет использования «перемешанного» алфавита. Однако наиболее стойким к расшифрованию сообщений из данного класса шифров является шифр полиалфавитной замены, в котором применяется несколько алфавитов, поочередно используемых для замены букв открытого текста.

Разновидностью шифрования с использованием полиалфавитной замены знаков сообщения является метод Вижинера (или шифр Вижинера), в котором важную роль играет ключевое слово.

Приведем в качестве примера программу шифрования текста сообщения с помощью шифра Вижинера. Программа может быть применена для создания шифротекстов с последующей передачей их в одноключевых криптосистемах.

Математическая постановка такой задачи заключается в следующем. Множество из 26 алфавитов, для английского текста (по числу букв), формируется последовательным циклическим сдвигом букв исходного алфавита (аналогично принципу формирования шифра Цезаря). Совокупность всех алфавитов образует так называемую таблицу Вижинера.

При шифровании буквы ключевого слова определяют выбор конкретного сдвинутого алфавита, используемого при замене соответствующей буквы сообщения.

Процесс шифрования может быть описан как процесс суммирования по модулю 26 номеров соответствующих друг другу букв открытого текста и ключевого слова.

и данном случае для уяснения принципа получения криптограмм с использованием шифра Вижинера применим ключевое слово и один алфавит английского языка.

Каждой букве алфавита сопоставим цифру (A $^{\Omega\Omega}$ 0, B $^{\Omega\Omega}$ 1, …, Z $^{\Omega\Omega}$ 25). Ключевое слово k_i задается определенным количеством букв d и повторно записывается под шифруемым сообщением m_i. В дальнейшем в i-м столбце из двух букв буква сообщения m_i складывается по модулю 26 со стоящей под ней буквой ключевого слова k_i в виде:

$$g_i = m_i + k_i \bmod 26,$$

где g_i — буквы полученной криптограммы.

Расшифровка криптограммы осуществляется вычитанием ключевого слова по модулю 26. При $d = 1$ шифр Вижинера является шифром Цезаря.

2. Примеры

Пример 1. Шифр Цезаря

Получим криптограмму с использованием шифра Цезаря с ключом $d = 1$ на базе английского алфавита, строчный регистр.

Исходное сообщение	i	n	f	o	r	m	f	t	i	o	n
Криптограмма	j	o	g	p	s	n	g	u	j	p	o

Для русского языка с ключом $d = 10$

Исходное сообщение	И	Н	Ф	О	Р	М	А	Ц	И	Я
Криптограмма	Т	Ч	Ю	Ш	Ь	Ц	Й	А	Т	И

Пример 2. Шифр Вижинера

Получим криптограмму с использованием шифра Цезаря с ключевым словом «code» (ключи «c=2», «o=14», «d=3», «e=4») на базе английского алфавита, строчный регистр.

Исходное сообщение	i	n	f	o	r	m	f	t	i	o	n

Ключевое слово	c	o	d	e	c	o	d	e	c	o	d
Криптограмма	k	b	i	s	t	a	i	x	k	c	q

Для русского языка с ключевым словом «код» (ключи «к=10», «о=14», «д=4»).

Исходное сообщение	И	Н	Ф	О	Р	М	А	Ц	И	Я
Ключевое слово	К	О	Д	К	О	Д	К	О	Д	К
Криптограмма	Т	Ы	Ш	Ш	Ю	Р	Й	Д	М	И

3. Практика

1. Ознакомиться с теоретической частью работы.
2. Составьте алгоритмическое и программное обеспечение:
   1. Процедур шифрования и расшифрования с использованием шифра Цезаря при вводе с клавиатуры ключа и исходного или зашифрованного текста. Учтите регистр вводимого текста.
   2. Процедур шифрования и расшифрования с использованием шифра Цезаря при вводе с клавиатуры ключа и текстового файла. Учтите регистр вводимого текста.
   3. Процедур шифрования и расшифрования с использованием шифра Вижинера при вводе с клавиатуры ключа и исходного или зашифрованного текста. Учтите регистр вводимого текста.
   4. Процедур шифрования и расшифрования с использованием шифра Вижинера при вводе с клавиатуры ключа и текстового файла. Учтите регистр вводимого текста.
   5.
   6. Постройте программно таблицу Вижинера и выведите в файл.
   7. Для созданного программного обеспечения проведите тестирование не менее чем на 10 различных наборах данных.
3. Составить отчет и защитить работу.

Раздел 5. Электронная подпись

1. Опрос по теме

Электронная цифровая подпись и ее использование. Основные понятия и свойства. Аппаратно-программные средства защиты информации. Средства обеспечения конфиденциальности данных; средства идентификации и аутентификации пользователей.

2. Лабораторная работа 5

Электронно-цифровая подпись и приемы хеширования
Обмен ключами по Диффи-Хелману

1. Теория

Для защиты информации в вычислительных сетях используется такой элемент криптографического преобразования как шифрование, в котором всегда различают два элемента: ключ и алгоритм. При этом ключом является секретное состояние некоторых параметров алгоритма криптопреобразования сообщения.

На практике в зависимости от способа применения ключа различают 2 типа криптографических систем:

- Одноключевые (симметричные)
- Двухключевые (несимметричные)

В одноключевых системах, называемых традиционными, ключи шифрования и расшифрования (л.р.2) либо одинаковы, либо легко выводятся один из другого, обепечивая таким образом единый общий ключ. Такой ключ является секретные передается получателю сообщения только по защищенному каналу связи.

Однако при этом имеет место следующий парадокс: если для обмена ее секретного ключа используется защищенный канал, то нет необходимости шифровать конфиденциальные сообщения, гораздо проще отправить их по этому каналу.

Отмеченный парадокс может быть исключен использованием идеи Диффи и Хеллмана, которые предложили способ выработки секретного ключа без предварительного согласования между абонентами сети путем обмена информацией по открытому каналу. Этот способ был предложен Диффи и Хеллманом в 1976 году и опубликован в ряде работ по криптографии. Реализация такого способа привела к появлению открытого шифрования. Абонент сего открыто сообщал о том, каким образом зашифровать к нему сообщение, расшифровать же его мог только он сам.

Основную роль при выработке секретного ключа в данном случае играют математические операции, когда прямая операция сравнительно проста, а обратная — практически трудно реализуема.

Прямая операция: возвести основание a в степень p и взять остаток по модулю m вида:

$$L = a^p \bmod m.$$

Обратная операция: найти p, зная L, a и m.

Обратная операция (задача) при этом может быть решена простым перебором значений p, но практически не решается при больших значениях p.

В предлагаемом алгоритме выработки секретного ключа известны основание a и mod m.

Отправитель сообщения с помощью генератора случайных чисел (ГСЧ) получает случайное число X ($1 < x < m$), вычисляет значение $L_0 = a^y \bmod m$ и посылает L_0 получателю.

Получатель принимает L_0 вырабатывает с помощью своего ГСЧ случайное число Y ($1 < y < m$), вычисляет значение $L_p = a^y \bmod m$ и посылает L_p отправителю.

Отправитель принимает Lp, вычисляет $K_0 = Lp^x = a^{yx} \bmod m$.

Получатель вычисляет $K_p = L_0^y = a^{yx} \bmod m$.

Так как $K_0 = K_p$., то это число и является общим секретным ключом. Злоумышленник, перехватив L_0 и L_p , не знает случайных чисел x и y и не сможет расшифровать исходный текст сообщения.

2. Практика

1. Составьте программное обеспечение, реализующее алгоритм обмена ключами. Ключи должны автоматически формироваться в файлы. Должна быть обеспечена наглядность выполнения алгоритма. Для созданного программного обеспечения проведите тестирование не менее чем на 10 различных наборах данных.
2. Составить программу шифрования методом контрольных сумм.
3. Составить программу шифрования методом хеширования с применением гаммирования.
4. Составить отчет и защитить работу.

Раздел 6. Компьютерная стеганография

1. Опрос по теме

Компьютерная стеганография и ее применение. Базовые понятия стеганографии Модель стеганографической системы. Понятие контейнера, виды контейнеров. Методы сокрытия информации в мультимедийных файлах. Направления развития компьютерной стеганографии.

2. Лабораторная работа 6

Стеганография. Внедрение информации на HTML-странице

1. Теория

Идея сокрытия информации на HTML-странице состоит в следующем. Буквы заменяют числами в соответствии с некоторой кодовой таблицей. Числа переводят из десятичной системы счисления в двоичную систему счисления. Скрываемый текст размещают после закрывающего тега </html>, причем вместо единиц записывают пробелы, а вместо нулей – символы табуляции. Эти символы на странице не видны (электронный аналог симпатических чернил).

Предположим, что нужно секретно передать через Интернет слово «Щит». Буквам этого слова соответствуют три десятичных числа: 217, 232 и 242. В двоичной системе счисления эти числа будут выглядеть так: 11011001, 11101000, 11110010.

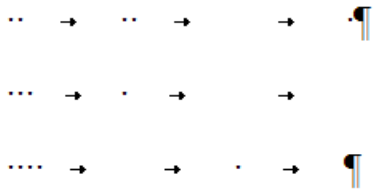
Заменив единицы и нули соответственно на пробелы и символы табуляции, скрытый текст размещают на HTML-странице ниже последнего тега. Увидеть закодированный текст можно с помощью текстового редактора MS Word, включив режим «Непечатаемые знаки».

В качестве примера рассмотрим HTML-код простейшей веб-страницы.

```
<html>
<head>
<title>
</head>
<body>
Простейшая HTML-страница
</body>
</html>
```

Если текст HTML-кода загрузить в редактор MS Word, то можно увидеть скрытую информацию:

```
<html>
<head>
<title>
</head>
<body>
Простейшая HTML-страница
</body>
</html>
```



Последние три строчки содержат скрытую информацию, причем пробелы отображаются здесь точками, символ табуляции – стрелкой. Символ ¶ является

служебным и обозначает конец абзаца и перевод строки. Предварительное шифрование текста позволяет повысить криптостойкость передаваемого сообщения.

2. Практика

1. Ознакомиться с теоретической частью работы.
2. Используя блокнот Notepad, создать HTML-страницу. В соответствии с вариантом выполнить кодирование текста и поместить код в контейнер, в качестве которого используется HTML-страница.
3. Составить отчет и защитить работу.

Раздел 7. Построение защищенных экономических систем

1. Опрос по теме

Основные технологии построения защищенных систем.
Для каждого из рассматриваемых процессов, таких как извлечение информации, транспортирование, обработка, хранение, представление и использование информации, дается подробная характеристика с раскрытием моделей и современного состояния. Детально раскрываются базовые информационные технологии, к которым отнесены: мультимедиа технологии, геоинформационные, технологии защиты информации, CASE-технологии, телекоммуникационные технологии, технологии искусственного интеллекта, технологии программирования, облачные технологии, технология больших данных. Приводится анализ прикладных информационных технологий для различных предметных областей, в частности, технологий корпоративного управления. Дается анализ и приводятся рекомендации по использованию программных, технических и методических средств информационных технологий. Излагается технология построения информационных систем, что особо актуально для формирования профессионалов-разработчиков. Приводятся основы системного подхода применительно к задачам построения информационных систем.
Методы идентификации и проверки подлинности пользователей информационных систем. Основные технологии построения защищенных ЭИС. Место ИБ экономических систем в национальной безопасности страны. Концепция ИБ. Особенности работы с персоналом, владеющим конфиденциальной информацией. Технологические основы обработки конфиденциальных документов. ISO/IEC 27005:2011 и ГОСТ Р ИСО/МЭК 27005–2010 – управление рисками ИБ. ISO/IEC 27006:2011 и ГОСТ Р ИСО/МЭК 27006–2008 – требования к органам, осуществляющим аудит и сертификацию СУИБ. ISO/IEC 27007:2011 и ISO/IEC 27008:2011 – руководства по аудиту СУИБ и средств управления ИБ, реализованных в СУИБ. ISO/IEC 27011:2008 – руководство по управлению ИБ для телекоммуникационных компаний на основе ISO/IEC 27002.

2. Лабораторная работа 7

Шифр RSA

1. Теория

Защита данных с помощью криптографического преобразования является эффективным решением проблемы их безопасности. Зашифрованные данные доступны лишь тем, кто знает, как их расшифровать, то есть тем, кто обладает соответствующим ключом шифрования.

Одним из наиболее перспективных криптографических стандартов на шифрование данных являются системы с открытым ключом. В таких системах для шифрования используется один ключ, а для расшифрования другой. Первый ключ является открытым и может быть опубликован для шифрования своей информации любым пользователем сети. Получатель зашифрованной информации для расшифровки данных использует

второй ключ, являющийся секретным. При этом должно соблюдаться следующее условие: секретный ключ не может быть определен из опубликованного открытого ключа.

Криптографические системы с открытым ключом используют необратимые или односторонние функции, обладающие важным свойством: при заданном значении x относительно просто вычислить значение $f(x)$, однако, если $y = f(x)$, то нет простого пути для вычисления значения x, то есть очень трудно рассчитать значение обратной функции $1 // f(y)$.

В настоящее время широко используется метод криптографической защиты данных с открытым ключом RSA, получившим название по начальным буквам фамилий его изобретателей (Rivest, Shamir, Adleman). На основе метода RSA разработаны алгоритмы шифрования, успешно применяемые для защиты информации. Он обладает высокой криптостойкостью и может быть реализован при использовании относительно несложных программных и аппаратных средств. Данный метод позволил решить проблему обеспечения персональных подписей в условиях безбумажной передачи и обработки данных. Описание схем формирования шифротекста в алгоритмах типа RSA приведено в различной литературе.

Использование метода RSA для криптографической защиты информации может быть пояснено с помощью структурной схемы, представленной на рисунке.

Функционирование криптосистемы на основе метода RSA предполагает формирование открытого и секретного ключей. С этой целью необходимо выполнить следующие математические операции:

- Выбираем два больших простых числа p и q, понимая под простыми числами такие числа, которые делятся на само себя и число 1,
- Определяем $n = p \times q$,
- Вычисляем число $k = (p-1)(q-1)$,
- Выбираем большое случайное число d, взаимно простое с числом k (взаимно простое число — это число, которое не имеет ни одного общего делителя, кроме числа 1)
- Определяем число e, для которого истинным является соотношение

$$(e \times d) \bmod k = 1$$

- Принимаем в качестве открытого ключа пару чисел $\{e, n\}$
- Формирование секретного ключа в виде пары чисел $\{d, n\}$

Для зашифровки передаваемых данных с помощью открытого ключа $\{e, n\}$ необходимо выполнить операции:

- Разбить шифруемый текст на блоки, каждый из которых может быть представлен в виде чисел $M(i) = 0,1,..., n-1$
- Зашифровать текст в виде последовательности чисел $M(i)$ по формуле

$$C(i) = (M(i)^e) \bmod n$$

- Расшифрование шифротекста производится с помощью секретного ключа $\{d, n\}$ при выполнении следующих вычислений:

$$M(i) = (C(i)^d) \bmod n$$

В результате получаем последовательность чисел $M(i)$, представляющих исходные данные. На практике при использовании метода RSA длина p и q составляет 100 и более десятичных знаков, что обеспечивает высокую криптостойкость шифротекста.

2. Практика

1. Ознакомиться с теоретической частью работы.

2. Составьте программное обеспечение, реализующее алгоритм RSA. Исходные данные должны передаваться через файлы: файл с открытым ключом, закрытым ключом и шифруемая информация. Для созданного программного обеспечения проведите тестирование не менее чем на 10 различных наборах данных.

3. Составить отчет и защитить работу.

Раздел 8. Защищенные компьютерные системы

1. Опрос по теме

Использование защищенных компьютерных систем. Защита операционной системы и других системных программных средств. Организация доступа в локальных сетях. ISO/IEC 27013 – руководство по интегрированному внедрению стандартов ISO/IEC 20000 и 27001. ISO/IEC 27014 – инфраструктура руководства ИБ. ISO/IEC 27015 – руководство по управлению ИБ для финансовых сервисов. ISO/IEC 27031:2011 – руководство по готовности информационных и телекоммуникационных технологий для обеспечения непрерывности бизнеса.

2. Лабораторная работа 8

Организационно-правовое обеспечение программного обеспечения

1. Теория

Целью работы является закрепление теоретических знаний в области правового обеспечения информационной безопасности.

Вариант задания

1. Назовите основные положения Доктрины информационной безопасности РФ.
2. Назовите составляющие правового института государственной тайны.
3. В каких случаях нельзя относить информацию к государственной тайне?
4. Какая система обозначения сведений, составляющих государственную тайну, принята в РФ?
5. Назовите группу видов ущерба, возникающего при утечке сведений, составляющих государственную тайну.
6. Дайте определение системы защиты государственной тайны и укажите ее составляющие.
7. Что в соответствии с законодательством РФ представляет собой засекречивание информации?
8. Перечислите основные принципы засекречивания информации.
9. Что понимается под профессиональной тайной?
10. Какие виды профессиональных тайн вам известны?
11. В чем заключается разница между понятиями «конфиденциальная информация» и «тайна»?
12. В чем состоит сложность служебной тайны с точки зрения определения ее правового режима?
13. Что представляет собой электронная цифровая подпись?
14. Каковы основные особенности правового режима электронного документа?
15. Назовите основные ограничения на использование электронных документов.

2. Практика

1. Изучить литературу и учебные материалы по теме (Конституция РФ, Доктрина информационной безопасности РФ и федеральные законы в области информационной безопасности, правовые режимы защиты информации).
2. Ответить на контрольные вопросы.
3. Оформить отчет, содержащий краткую информацию по контрольным вопросам.

3. Контрольная работа 1

1. Определение понятий «Информация» «Информационная безопасность», «Субъекты информационных отношений»
2. Категорирование информации

3. Задание требований к информационной безопасности организации
4. Понятие угрозы информационной безопасности. Классификация угроз ИБ
5. Состав средств и мер защиты информации. Классификация средств и мер защиты информации
6. Объект и субъект защиты информации
7. Каналы утечки информации. Классификация каналов утечки информации
8. Модель нарушителя информационной безопасности
9. Классификация нарушителей информационной безопасности
10. Компьютерные «Вирусы». Их виды
11. Способы борьбы с компьютерными вирусами
12. Определение понятия «Система информационной безопасности»
13. Элементы системы информационной безопасности
14. Определение понятия «Государственная тайна»
15. Регулирование правовых отношений в области защиты государственной тайны
16. Модели безопасности их применение
17. Место ИБ экономических систем в национальной безопасности страны
18. Основы конфиденциального документооборота
19. Особенности работы с персоналом, владеющим конфиденциальной информацией
20. Принципы построения защищенных компьютерных систем
21. Элементы операционной системы
22. Управление доступом пользователей в операционных системах
23. Парольная политика популярных операционных систем
24. Состав локально-вычислительных сетей
25. Коммутаторы, концентраторы, маршрутизаторы
26. Организация доступа в локальных сетях
27. Контроль сетевых подключений
28. Управление сетевой маршрутизацией
29. Управление доступом к компьютерам
30. Система управления паролями
31. Управление доступом к приложениям
32. Управление доступом к библиотекам исходных текстов программ

Перечень вопросов к экзамену

1. Определение понятий «Информация» «Информационная безопасность», «Субъекты информационных отношений»
2. Категорирование информации
3. Задание требований к информационной безопасности организации
4. Виды возможных нарушений информационной системы. Общая классификация информационных угроз
5. Угрозы ресурсам компьютерной безопасности. Угрозы, реализуемые на уровне локальной компьютерной системы. Человеческий фактор
6. Угрозы компьютерной информации, реализуемые на аппаратном уровне
7. Удаленные атаки на компьютерные системы. Причины уязвимостей компьютерных сетей
8. Состав средств и мер защиты информации. Классификация средств и мер защиты информации
9. Объект и субъект защиты информации
10. Каналы утечки информации. Классификация каналов утечки информации
11. Модель нарушителя информационной безопасности
12. Классификация нарушителей информационной безопасности

13. Компьютерные вирусы. История. Определение по УК РФ
14. Определение понятия «Система информационной безопасности»
15. Элементы системы информационной безопасности
16. Определение понятия «Государственная тайна»
17. Регулирование правовых отношений в области защиты государственной тайны
18. Модели безопасности их применение
19. Место ИБ экономических систем в национальной безопасности страны
20. Основы конфиденциального документооборота
21. Особенности работы с персоналом, владеющим конфиденциальной информацией
22. Принципы построения защищенных компьютерных систем
23. Элементы операционной системы
24. Управление доступом пользователей в операционных системах
25. Парольная политика популярных операционных систем
26. Состав локально-вычислительных сетей
27. Коммутаторы, концентраторы, маршрутизаторы
28. Организация доступа в локальных сетях
29. Контроль сетевых подключений
30. Управление сетевой маршрутизацией
31. Управление доступом к компьютерам
32. Система управления паролями
33. Управление доступом к приложениям
34. Управление доступом к библиотекам исходных текстов программ
35. Правовое урегулирование защиты информации. Стандарты ИБ
36. Защита данных криптографическими методами. Методы шифрования
37. Защита данных криптографическими методами. Алгоритмы шифрования

Таблица 9 – Примеры оценочных средств с ключами правильных ответов

№ п/п	Тип задания	Формулировка задания	Правильный ответ	Время выполнения (в минутах)
ОПК-2. Способен понимать принципы работы современных информационных технологий и программных средств, в том числе отечественного производства, и использовать их при решении задач профессиональной деятельности				
1.	Задание закрытого типа	Существуют три причины использования распределенных атак злоумышленником. Какая из перечисленных лишняя: а. сокрытие. б. мощность. в. сбор информации. г. отсутствие последствий после вторжения	г	2
2.		Укажете два основных метода анализа, связанных с выявлением атак в системах обнаружения вторжений: а. сигнатурный метод и метод, связанный с выявлением аномального поведения. б. сигнальный метод и метод, связанный с выявлением	а	2

№ п/п	Тип задания	Формулировка задания	Правильный ответ	Время выполнения (в минутах)
		аномального поведения. в. сигнатурный и сигнальный методы. г. структурный и сигнальный методы.		
3.		Если пользователи создают свои собственные пароли, каких рекомендаций они должны придерживаться (выберите все возможные варианты)? a) использовать максимально возможное количество символов в пароле; b) использовать в качестве пароля имя супруга/супруги, ребенка или кличку собаки (чтобы не забыть пароль); c) использовать хотя бы одну прописную букву, один символ нижнего регистра, одну цифру и один допустимый не алфавитно-цифровой символ; d) использовать пароль, который трудно угадать по смыслу.	в, г	2
4.		Уязвимость информации — это: a) Возможность возникновения на каком-либо этапе жизненного цикла КС такого ее состояния, при котором создаются условия для реализации угроз безопасности информации. b) Событие или действие, которое может вызвать изменение функционирования КС, связанное с нарушением защищенности обрабатываемой в ней информации. c) Это действие, предпринимаемое нарушителем, которое заключается в поиске и использовании той или иной уязвимости.	б	2

№ п/п	Тип задания	Формулировка задания	Правильный ответ	Время выполнения (в минутах)
5.		Под угрозой безопасности информации в компьютерной системе (КС) понимают: а) возможность возникновения на каком-либо этапе жизненного цикла КС такого ее состояния, при котором создаются условия для реализации угроз безопасности информации. б) Событие или действие, которое может вызвать изменение функционирования КС, связанное с нарушением защищенности обрабатываемой в ней информации. с) действие, предпринимаемое нарушителем, которое заключается в поиске и использовании той или иной уязвимости	с	2
6.	Задание открытого типа	Основные задачи при эксплуатации механизмов аутентификации	При эксплуатации механизмов аутентификации основными задачами являются: генерация или изготовление идентификаторов, их учет и хранение, передача идентификаторов пользователю и контроль над правильностью выполнения процедур аутентификации в КС.	3
7.		Что понимается под системой защиты от несанкционированного использования и копирования	Под системой защиты от несанкционированного использования и копирования понимается комплекс программных или программно-аппаратных средств, предназначенных для усложнения или запрещения	3

№ п/п	Тип задания	Формулировка задания	Правильный ответ	Время выполнения (в минутах)
			нелегального распространения, использования и (или) изменения программных продуктов и иных информационных ресурсов.	
8.		Что должен выполнить для защиты инсталлируемой программы от копирования при помощи криптографических методов инсталлятор программы?	Для защиты инсталлируемой программы от копирования при помощи криптографических методов инсталлятор программы должен выполнить следующие функции: − анализ аппаратно-программной среды компьютера, на котором должна будет выполняться инсталлируемая программа, и формирование на основе этого анализа эталонных характеристик среды выполнения программы; − запись криптографически преобразованных эталонных характеристик аппаратно-программной среды компьютер на винчестер.	3
9.		Основные компоненты системы защиты программных продуктов от несанкционированного копирования	Основные компоненты системы защиты программных продуктов от несанкционированного копирования: модуль проверки	3

№ п/п	Тип задания	Формулировка задания	Правильный ответ	Время выполнения (в минутах)
			ключевой информации (некопируемой метки на дистрибутивном диске, уникального набора характеристик компьютера, идентифицирующей информации для легального пользователя) – может быть добавлен к исполнимому коду защищаемой программы по технологии компьютерного вируса, в виде отдельного программного модуля или в виде отдельной функции проверки внутри защищаемой программы; модуль защиты от изучения алгоритма работы системы защиты; модуль согласования с работой функций защищаемой программы в случае ее санкционированного использования; модуль ответной реакции в случае попытки несанкционированного использования (как правило, включение такого модуля в состав системы защиты нецелесообразно по морально-этическим соображениям).	
10.		Основные требования, предъявляемые к системе защиты от копирования	Основные требования, предъявляемые к системе защиты от копирования: обеспечение	3

№ п/п	Тип задания	Формулировка задания	Правильный ответ	Время выполнения (в минутах)
			некопируемости дистрибутивных дисков стандартными средствами (для такого копирования нарушителю потребуется тщательное изучение структуры диска с помощью специализированных программных или программно-аппаратных средств); обеспечение невозможности применения стандартных отладчиков без дополнительных действий над машинным кодом программы или без применения специализированных программно-аппаратных средств (нарушитель должен быть специалистом высокой квалификации); обеспечение некорректного дисассемблирования машинного кода программы стандартными средствами (нарушителю потребуется использование или разработка специализированных дисассемблеров); обеспечение сложности изучения алгоритма распознавания индивидуальных	

№ п/п	Тип задания	Формулировка задания	Правильный ответ	Время выполнения (в минутах)
			параметров компьютера, на котором установлен программный продукт, и его пользователя или анализа применяемых аппаратных средств защиты (нарушителю будет сложно эмулировать легальную среду запуска защищаемой программы).	
ОПК-3. Способен решать стандартные задачи профессиональной деятельности на основе информационной и библиографической культуры с применением информационно- коммуникационных технологий и с учетом основных требований информационной безопасности				
11.	Задание закрытого типа	К угрозам информационной безопасности со стороны человеческого фактора НЕ относятся: 1. Действия уволенных или недовольных сотрудников 2. Анализаторы протоколов 3. Халатность 4. Низкая квалификация работников	2	2
12.		К техническим средствам обеспечения информационной безопасности и защиты информации относятся: 1. Недопущение ведения важных работ одним человеком 2. Резервирование особо важных компьютерных подсистем 3. Защита авторских прав программистов	2	2
13.		К техническим угрозам информационной безопасности	3	2

№ п/п	Тип задания	Формулировка задания	Правильный ответ	Время выполнения (в минутах)
		НЕ относится: 1. Ошибки в программном обеспечении 2. Сетевые атаки, в том числе DoS- и DDoS-атаки 3. Промышленный шпионаж 4. Компьютерные вирусы, черви, троянские кони		
14.		К организационным средствам обеспечения информационной безопасности и защиты информации относятся: 1. Совершенствование законодательства и судопроизводства 2. Тщательный подбор персонала 3. Установка средств обнаружения и тушения пожара, обнаружения утечек воды	2	2
15.	Задание комбинированного типа	Цели защиты информации (указать несколько правильных ответов): 1. Целостность данных 2. Конфиденциальность данных 3. Доступность данных 4. Открытость данных	Целями защиты информации являются: - целостность данных гарантирует, что они не были изменены, подменены или уничтожены в результате злонамеренных действий или случайностей; - конфиденциальность данных — это статус, предоставленный данным и определяющий требуемую степень их защиты.	8

№ п/п	Тип задания	Формулировка задания	Правильный ответ	Время выполнения (в минутах)
			Конфиденциальная информация должна быть известна только допущенным и прошедшим проверку (авторизацию) субъектам информационной системы (пользователям, процессам, программам); - доступность данных, условием работы с данными является доступ пользователя к ним. Под доступом к информации понимается ознакомление с ней и ее обработка, в частности, копирование, модификация, уничтожение. Различают санкционированный и несанкционированный доступ. Санкционированный доступ — это доступ в соответствии с установленными правилами разграничения доступа. Несанкционированный доступ нарушает эти правила.	
16.	Задание открытого типа	Какие меры относится к правовым мерам, направленным на обеспечение информационной безопасности и защиты информации?	Правовые нормы: разработка норм, устанавливающих ответственность за компьютерные преступления; защита авторских прав программистов; совершенствование законодательства и	4

№ п/п	Тип задания	Формулировка задания	Правильный ответ	Время выполнения (в минутах)
			судопроизводства; общественный контроль за разработчиками компьютерных систем и приятие международных договоров, регламентирующих эту деятельность.	
17.		Какие меры относится к техническим мерам, направленным на обеспечение информационной безопасности и защиты информации?	Технические меры: защита от несанкционированного доступа к информационной системе; резервирование особо важных компьютерных подсистем; организация вычислительных сетей с возможностью перераспределения ресурсов при нарушении в работе отдельных звеньев; установка средств обнаружения и тушения пожара, обнаружение утечек воды; принятие конструкционных мер защиты от хищений, диверсий, взрывов; установка резервного электропитания, оснащение помещений замками, сигнализацией.	4
18.		Какие меры относится к организационным мерам, направленным на обеспечение информационной безопасности и защиты информации?	Организационные меры: охрана вычислительного центра (ВЦ); тщательный подбор персонала; недопущение ведения важных работ одним	4

№ п/п	Тип задания	Формулировка задания	Правильный ответ	Время выполнения (в минутах)
			человеком; наличие плана восстановления работоспособности ВЦ после выхода его из строя; обслуживание ВЦ сторонней организацией или лицами, незаинтересованными в сокрытии факторов нарушения работы центра; выбор места расположения центра.	
19.		Согласно Федеральному закону «Об информации, информационных технологиях и о защите информации» не может быть ограничен доступ к: 1. Информации о состоянии окружающей среды 2. Персональным данным граждан (физических лиц) 3. Информации о деятельности государственных органов и органом местного самоуправления, а также об использовании бюджетных средств	Согласно Федеральному закону «Об информации, информационных технологиях и о защите информации» не может быть ограничен доступ к информации о состоянии окружающей среды, информации о деятельности государственных органов и органом местного самоуправления, а также об использовании бюджетных средств	4
20.	Задание комбинированного типа	Ныне действующим стандартом симметричного шифрования является: 1) DES; 2) ГОСТ 28147-89; 3) AES.	Американский стандарт симметричного шифрования DES (Data Encryption Standard) был принят в 1977 г., является представителем блочных шифров, ныне устарел из-за своего короткого ключа, Российский алгоритм шифрования ГОСТ	2

№ п/п	Тип задания	Формулировка задания	Правильный ответ	Время выполнения (в минутах)
			28147-89 является также примером DES-подобных криптосистем, формировался с учетом недостатков алгоритма DES, но длинный ключ обусловливает медлительность российского алгоритма. Ныне действующий стандарт шифрования AES является новым стандартом блочного шифра, имеет высокую скорость шифрования на всех платформах в программной и в аппаратной реализации, минимальные требования к ресурсам, широкие возможности для распараллеливания вычислений и др.	

Полный комплект оценочных материалов по дисциплине (модулю) (фонд оценочных средств) хранится в электронном виде на кафедре, утверждающей рабочую программу дисциплины (модуля), и в Центре мониторинга и аудита качества обучения.

7.4. Методические материалы, определяющие процедуры оценивания знаний, умений, навыков и (или) опыта деятельности

Методические рекомендации по выполнению лабораторных и контрольных работ, проведению экзамена

Критерии оценки обсуждения вопросов по теме:

– оценка «отлично» выставляется обучающемуся, если студент продемонстрировал глубокие знания теоретического материала и умение их применять, обоснованно изложил свои мысли, сделал необходимые выводы;

– оценка «хорошо» выставляется обучающемуся, если студент продемонстрировал глубокие знания теоретического материала и умение их применять, обоснованно изложил свои мысли, сделал необходимые выводы, допущены некоторые неточности, имеется одна негрубая ошибка.

– оценка «удовлетворительно» выставляется обучающемуся, если студент ответил на вопросы преимущественно верно, имеются затруднения в формулировке выводов, имеются одна или две негрубые ошибки;

– оценка «неудовлетворительно» выставляется обучающемуся, если студент не дал ответы на поставленные вопросы, обоснования неверные, либо дан верный ответ без его обоснования, сделаны грубые ошибки.

Отчет по лабораторной работе

Отчет по лабораторной работе представляется в электронном виде. Защита отчета проходит в форме доклада студента по выполненной работе и ответов на вопросы преподавателя. В случае, если оформление отчета и поведение студента во время защиты соответствуют указанным требованиям, студент получает максимальное количество баллов.

Основаниями для снижения количества баллов в диапазоне от max до min являются:

- отсутствие списка использованной литературы,
- небрежное выполнение,
- отсутствие выводов.

Отчет не может быть принят и подлежит доработке в случае:

- отсутствия необходимых разделов,
- отсутствия необходимого графического материала,
- неверных результатов расчета.

В отчете по выполненной лабораторной работе должны быть указаны:

- тема лабораторной работы,
- пакет документов в соответствии с темой лабораторной работы,
- использованная литература.

Критерии оценки:

– оценка «отлично» выставляется обучающемуся, если студент продемонстрировал глубокие знания теоретического материала и умение их применять, обоснованно изложил свои мысли, сделал необходимые выводы;

– оценка «хорошо» выставляется обучающемуся, если студент продемонстрировал глубокие знания теоретического материала и умение их применять, обоснованно изложил свои мысли, сделал необходимые выводы, допущены некоторые неточности, имеется одна негрубая ошибка;

– оценка «удовлетворительно» выставляется обучающемуся, если студент ответил на вопросы преимущественно верно, имеются затруднения в формулировке выводов, имеются одна или две негрубые ошибки;

– оценка «неудовлетворительно» выставляется обучающемуся, если студент не дал ответы на поставленные вопросы, обоснования неверные, либо дан верный ответ без его обоснования, сделаны грубые ошибки, отсутствуют знания по основам математики.

Контрольные работы

Контрольная работа состоит из 2-х заданий.

Основаниями для снижения оценки за задание являются:

- ошибки в объяснениях и комментариях при верно выполненном задании;
- неполный ответ для теоретический заданий;
- небрежное выполнение;
- многократное переписывание контрольной работы.

Задание не может быть засчитано, если:

- даны два неверных ответа на теоретические вопросы.

Метод "золотого сечения"

Критерии оценки контрольных работ:

– оценка «отлично» выставляется обучающемуся, если студент продемонстрировал глубокие знания теоретического материала и умение их применять, обоснованно изложил свои мысли, сделал необходимые выводы и учел основные нормативно-правовые документы по информационной безопасности;

– оценка «хорошо» выставляется обучающемуся, если студент продемонстрировал глубокие знания теоретического материала и умение их применять, обоснованно изложил свои мысли, сделал необходимые выводы и учел основные нормативно-правовые

документы по информационной безопасности, допущены некоторые неточности, имеется одна негрубая ошибка.

– оценка «удовлетворительно» выставляется обучающемуся, если студент ответил на вопросы преимущественно верно, имеются затруднения в формулировке выводов, имеются одна или две негрубые ошибки, учтены не все нормативно-правовые документы по информационной безопасности;

– оценка «неудовлетворительно» выставляется обучающемуся, если студент не дал ответы на поставленные вопросы, обоснования неверные, либо дан верный ответ без его обоснования, сделаны грубые ошибки, отсутствуют знания нормативно-правовых документов по информационной безопасности.

Критерии оценки теста:

- оценка «отлично» выставляется студенту, если он умеет безошибочно самостоятельно обрабатывать и интерпретировать данные при решении задач, как в стандартной, так и в нестандартной формулировке;
- оценка «хорошо» выставляется студенту, если он умеет безошибочно самостоятельно обрабатывать и интерпретировать данные при решении задач в стандартной ситуации или за верное решение 75% - 89% заданий теста;
- оценка «удовлетворительно» выставляется студенту, если он умеет при решении задач обрабатывать данные с опорой на справочные материалы и помощь преподавателя, верно выполняя при этом 60% - 74% работы.
- оценка «неудовлетворительно» выставляется студенту, если он не умеет правильно обрабатывать данные, выполнил менее 60% заданий теста.
- оценка «зачтено» выставляется студенту, если тест студента оценен не ниже чем «удовлетворительно»;
- оценка «не зачтено», если тест оценен ниже чем «удовлетворительно».

Экзамен

Экзамен заключается в письменном ответе на 2 теоретических вопроса и устном собеседовании по каждому теоретическому вопросу.

Основаниями для снижения оценки за теоретический вопрос являются:

- небрежное выполнение;
- неполный ответ;
- наличие мелких неточностей или незначительных искажений фактов;
- неточные объяснения при собеседовании;
- отсутствие ответов на заданные при собеседовании вопросы.

В соответствии с балльно-рейтинговой системой БАРС по дисциплине на экзамен отводится 100 баллов (40 баллов на текущие формы контроля, 10 баллов на бонусы и 50 баллов отводится на экзамен),

Оценивание студентов на экзамене осуществляется в соответствие с требованиями и критериями 100-балльной шкалы. Учитываются как результаты текущего контроля, так и знания, навыки и умения, непосредственно показанные студентами в ходе экзамена.

Критерии оценок на экзамене:

40-50 баллов – студент глубоко понимает пройденный материал, отвечает четко и всесторонне, умеет оценивать факты, самостоятельно рассуждает, отличается способностью обосновать выводы и разъяснять их в логической последовательности.

35-39 баллов – студент глубоко понимает пройденный материал, отвечает четко и всесторонне, умеет оценивать факты, самостоятельно рассуждает, отличается способностью обосновать выводы и разъяснять их в логической последовательности, но допускает отдельные неточности.

25-34 балла – студент глубоко понимает пройденный материал, отвечает четко и всесторонне, умеет оценивать факты, самостоятельно рассуждает, отличается

способностью обосновать выводы и разъяснять их в логической последовательности, но допускает некоторые ошибки общего характера.

20-24 балла – студент хорошо понимает пройденный материал, но не может теоретически обосновать некоторые выводы.

15-19 баллов – студент отвечает в основном правильно, но чувствуется механическое заучивание материала. 1

1-14 баллов – в ответе студента имеются существенные недостатки, материал охвачен «половинчато», в рассуждениях допускаются ошибки. 1

0 баллов – ответ студента правилен лишь частично, при разъяснении материала допускаются серьезные ошибки.

6-9 баллов – студент имеет общее представление о теме, но не умеет логически обосновать свои мысли.

1-5 баллов – студент имеет лишь частичное представление о теме. 0 баллов – нет ответа.

Таблица 10.Технологическая карта рейтинговых баллов по дисциплине (модулю)

№ п/п	Контролируемые мероприятия	Количество мероприятий / баллы	Максимальное количество баллов	Срок представления
Основной блок				
1.	*Ответ на занятии*	18/1	18	По расписанию
2.	*Выполнение лабораторной работы*	8/2	16	
3.	*Выполнение контрольной работы*	1/6	6	
Всего			**40**	-
Блок бонусов				
1.	*Посещение занятий без пропусков*	1	3	
2.	*Своевременное выполнение всех заданий*	1	3	
3.	*Активность студента на занятии*	1	4	
Всего			**10**	-
Дополнительный блок				
1.	*Экзамен*		50	
Всего			**50**	-
ИТОГО			**100**	-

Таблица 11. Система штрафов (для одного занятия)

Показатель	Балл
Опоздание на занятие	- 1
Нарушение учебной дисциплины	- 1
Неготовность к занятию	- 2
Пропуск занятия без уважительной причины	- 2

Таблица 12. Шкала перевода рейтинговых баллов в итоговую оценку за семестр по дисциплине (модулю)

Сумма баллов	Оценка по 4-балльной шкале	
90–100	5 (отлично)	зачтено
85–89	4 (хорошо)	

Сумма баллов	Оценка по 4-балльной шкале	
75–84		
70–74		
65–69	3 (удовлетворительно)	
60–64		
Ниже 60	2 (неудовлетворительно)	незачтено

При реализации дисциплины (модуля) в зависимости от уровня подготовленности обучающихся могут быть использованы иные формы, методы контроля и оценочные средства, исходя из конкретной ситуации.

8. УЧЕБНО-МЕТОДИЧЕСКОЕ И ИНФОРМАЦИОННОЕ ОБЕСПЕЧЕНИЕ ДИСЦИПЛИНЫ (МОДУЛЯ)

8.1. Основная литература

1. Шаньгин В.Ф., Информационная безопасность и защита информации/ Шаньгин В.Ф. - М. : ДМК Пресс, 2014. - 702 с. - ISBN 978-5-94074-768-0 -URL: http://www.studentlibrary.ru/book/ISBN9785940747680.html (ЭБС «Консультант студента»).

2. Защита информации: учебное пособие / Ю.М. Краковский - Ростов н/Д : Феникс, 2016. - (Высшее образование). - URL: http://www.studentlibrary.ru/book/ISBN9785222269114.html (ЭБС «Консультант студента»).

3. Комплексные (интегрированные) системы обеспечения безопасности [Электронный ресурс] / Ворона В.А., Тихонов В.А. - Вып. 7. - М. : Горячая линия - Телеком, 2013. - (Серия "Обеспечение безопасности объектов"). - URL: http://www.studentlibrary.ru/book/ISBN9785991202381.html (ЭБС «Консультант студента»).

4. Защита информации ограниченного доступа от утечки по техническим каналам / Г.А. Бузов - М. : Горячая линия - Телеком, 2015. - URL: http://www.studentlibrary.ru/book/ISBN9785991204248.html (ЭБС «Консультант студента»).

8.2. Дополнительная литература

21. Защита информации : Учебное пособие для вузов / Е.Б. Белов, В.П. Лось, Р.В. Мещеряков, А.А. Шелупанов. - М. : Горячая линия - Телеком, 2011. - URL: http://www.studentlibrary.ru/book/ISBN5935172925.html (ЭБС «Консультант студента»).

22. Информационная безопасность: защита и нападение / Бирюков А.А. - М. : ДМК Пресс, 2012. - URL: http://www.studentlibrary.ru/book/ISBN9785940746478.html (ЭБС «Консультант студента»).

23. Галатенко, В. А. Защита информации: курс лекций: учеб.пособие / В. А. Галатенко ; под ред. В. Б. Бетелина.- 2-е изд., испр. - М. : Интернет-Ун-т Информ. Технологий, 2004. - 264 с. (45 экз.)

24. Девянин П.Н. Модели безопасности компьютерных систем.-М.: Академия, 2005. 144 с. (50 экз.)

25. Садердинов А.А., Трайнев В.А., Федулов А.А. Информационная безопасность предприятия; уч. пособие. -2 изд. – М.: Издат.-торговая корпорация «Дашков и К», 2005, – 336 ч. (45 экз.)

26. Хорев П.Б. Методы и средства защиты информации в компьютерных системах : уч.пособие. – М.: Издат центр «Академия», 2005, – 256 с. (69 экз.)

27. Мельников, В.П. Информационная безопасность и защита информации : доп. УМО по ун-тскому политех. образованию в качестве учеб. пособия для студентов вузов, обучающихся по специальности 230201 "Информационные системы и технологии" / В. П. Мельников, Клейменов, С.А., Петраков, А.М. ; под ред. С.А. Клейменова. - 4-изд. ;

стер. - М. : Академия, 2009. - 336 с. - (Высшее профессиональное образование). - ISBN 978-5-7695-6150-4 : 306-46. (19 экз.)

8.3. Интернет-ресурсы, необходимые для освоения дисциплины (модуля)

1. **Электронно-библиотечная система (ЭБС) ООО «Политехресурс» «Консультант студента».** Многопрофильный образовательный ресурс «Консультант студента» является электронной библиотечной системой, предоставляющей доступ через сеть Интернет к учебной литературе и дополнительным материалам, приобретенным на основании прямых договоров с правообладателями. Каталог в настоящее время содержит около 15000 наименований. www.studentlibrary.ru.

9. МАТЕРИАЛЬНО-ТЕХНИЧЕСКОЕ ОБЕСПЕЧЕНИЕ ДИСЦИПЛИНЫ

Для проведения публичной защиты проектов, необходима мультимедийная аудитория с проектором.

Для проведения лабораторных занятий необходима компьютерная аудитория, в которой организован доступ к сети Интернет.

Учебные аудитории, библиотеки АГУ, центр мониторинга и аудита качества образования, компьютерные классы, мультимедийные аудитории.

Рабочая программа дисциплины (модуля) при необходимости может быть адаптирована для обучения (в том числе с применением дистанционных образовательных технологий) лиц с ограниченными возможностями здоровья, инвалидов. Для этого требуется заявление обучающихся, являющихся лицами с ограниченными возможностями здоровья, инвалидами, или их законных представителей и рекомендации психолого-медико-педагогической комиссии. Для инвалидов содержание рабочей программы дисциплины (модуля) может определяться также в соответствии с индивидуальной программой реабилитации инвалида (при наличии).