МИНОБРНАУКИ РОССИИ
АСТРАХАНСКИЙ ГОСУДАРСТВЕННЫЙ УНИВЕРСИТЕТ ИМ. В.Н. ТАТИЩЕВА

СОГЛАСОВАНО	УТВЕРЖДАЮ
Руководитель ОПОП	Заведующий кафедрой ЦТ
Гордеев И.И. Гордеев	А.Н. Марьенков
29 июня 2022 г.	29 июня 2022 г.

РАБОЧАЯ ПРОГРАММА ДИСЦИПЛИНЫ (МОДУЛЯ)

БЕЗОПАСНОСТЬ ИНФОРМАЦИОННЫХ СИСТЕМ И ТЕХНОЛОГИЙ

Составитель	**Марьенков А.Н., к.т.н., доцент каф. ЦТ, АГУ** **Выборнова О.Н., к.т.н, доцент каф. ИБ, АГУ**
Направление подготовки	**09.04.02 ИНФОРМАЦИОННЫЕ СИСТЕМЫ И ТЕХНОЛОГИИ**
Направленность (профиль) ОПОП	**ПРОЕКТИРОВАНИЕ И РАЗРАБОТКА СИСТЕМ ИСКУССТВЕННОГО ИНТЕЛЛЕКТА**
Квалификация (степень)	**магистр**
Форма обучения	**очная**
Год приема	**2022**
Курс	**2**

Астрахань – 2022 г.

1. ЦЕЛИ И ЗАДАЧИ ОСВОЕНИЯ ДИСЦИПЛИНЫ

1.1. Целями освоения дисциплины «Безопасность информационных систем и технологий» являются изучение основных принципов, методов и средств защиты информации в процессе ее обработки, передачи и хранения с использованием компьютерных средств в информационных системах.

1.2. Задачи освоения дисциплины:

- изучение принципов построения и сопровождения в процессе эксплуатации защищенных информационных систем;
- изучение особенностей обеспечения информационной безопасности в информационных системах;
- определение оценки эффективности обеспечения информационной безопасности.

2. МЕСТО ДИСЦИПЛИНЫ В СТРУКТУРЕ ОПОП

2.1. Учебная дисциплина Б1.В.Д.01.01 «Безопасность информационных систем и технологий» относится к элективным дисциплинам, направленных на приобретение профессиональных компетенций. Изучается в 3-м семестре.

2.2. Для изучения данной дисциплины студенту необходимы следующие знания, умения и навыки, формируемые предшествующими дисциплинами:

– Модели информационных процессов и систем

2.3. Перечень последующих учебных дисциплин, для которых необходимы знания, умения и навыки, формируемые данной учебной дисциплиной:

– Выпускная квалификационная работа;
– Производственная практика.

3. КОМПЕТЕНЦИИ ОБУЧАЮЩЕГОСЯ, ФОРМИРУЕМЫЕ В РЕЗУЛЬТАТЕ ОСВОЕНИЯ ДИСЦИПЛИНЫ

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

а) профессиональных (ПК):

ПК-8 - Способен разрабатывать и модернизировать программное и аппаратное обеспечение технологий и систем искусственного интеллекта с учетом требований информационной безопасности в различных предметных областях.

Таблица 1.
Декомпозиция результатов обучения

Код компетенции	Планируемые результаты освоения дисциплины (модуля)		
	Знать (1)	Уметь (2)	Владеть (3)
ПК-8 ПК-8.1. Разрабатывает программное и аппаратное обеспечение технологий и систем искусственного интеллекта для решения профессиональных задач с учетом требований информационной безопасности в различных предметных областях	ПК-8.1.1 новые научные принципы и методы разработки программного и аппаратного обеспечения технологий и систем искусственного интеллекта для решения профессиональных задач в различных предметных областях.	ПК-8.1.2. разрабатывать программное и аппаратное обеспечение технологий и систем искусственного интеллекта с учетом требований информационной безопасности для решения профессиональных задач в различных предметных областях.	ПК-8.1.3. навыками проведения оценки достоверности результатов работы систем, основанных на знаниях.
ПК-8 ПК-8.2. Модернизирует программное и аппаратное обеспечение технологий и систем искусственного интеллекта для решения	ПК-8.2.1 особенности модернизации программного и аппаратного обеспечения технологий и систем искусственного интеллекта для решения	ПК-8.2.2 модернизировать программное и аппаратное обеспечение технологий и систем искусственного интеллекта с учетом требований ин-	ПК-8.2.3. навыками проведения модернизации систем, основанных на знаниях.

профессиональных задач с учетом требований информационной безопасности в различных предметных областях.	профессиональных задач в различных предметных областях.	формационной безопасности для решения профессиональных задач в различных предметных областях.	

4. СТРУКТУРА И СОДЕРЖАНИЕ ДИСЦИПЛИНЫ

Объем дисциплины (модуля) 3 з. е., 108 часов, 54 часов выделено на контактную работу обучающихся с преподавателем (лекции – 18, лабораторные работы – 36), 54 часов – на самостоятельную работу обучающихся.

Таблица 2.

Структура и содержание дисциплины

№ п/п	Наименование раздела (темы)	Семестр	Неделя семестра	Контактная работа (в часах)			Самостоят. работа		Формы текущего контроля успеваемости
				Л	ПЗ	ЛР	КР	СР	
1	Тема 1. Цели и задачи информационной безопасности. Место информационной безопасности в национальной безопасности РФ	3	1-2	3		6		9	Лабораторная работа №1, устный опрос
2	Тема 2. Построение систем защиты информации в организации	3	3-4	3		6		9	Тест, устный опрос
3	Тема 3. Современные методики анализа и управления рисками информационной безопасности	3	5-6	3		6		9	Лабораторная работа №2, устный опрос
4	Тема 4. Основные программно-технические меры безопасности информации: идентификация и аутентификация; управление доступом	3	7-10	3		6		9	Контрольная работа №1, Лабораторная работа №3
5	Тема 5. Основные программно-технические меры безопасности информации: протоколирование, аудит, шифрование, контроль целостности, электронная подпись	3	11-14	3		6		9	Лабораторная работа №4, устный опрос
6	Тема 6. Основные технологии построения защищенных систем	3	15-18	3		6		9	Контрольная работа №2, Лабораторная работа №5, устный опрос
ИТОГО за 3 семестр		**108**		**18**		**36**		**54**	**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 в них компетенций

Темы, Разделы дисциплины	Кол-во часов	Компетенции	
		ПК 8	общее количество компетенций
Тема 1. Цели и задачи информационной безопасности. Место	18	+	1

информационной безопасности в национальной безопасности РФ			
Тема 2. Построение системы защиты информации в организации	18	+	1
Тема 3. Современные методики анализа и управления рисками информационной безопасности	18	+	1
Тема 4. Основные программно-технические меры безопасности информации: идентификация и аутентификация; управление доступом	18	+	1
Тема 5. Основные программно-технические меры безопасности информации: протоколирование, аудит, шифрование, контроль целостности, электронная подпись	18	+	1
Тема 6. Основные технологии построения защищенных систем	18	+	1
ИТОГО:	**108**		

Краткое содержание каждого раздела дисциплины

Тема 1. Цели и задачи информационной безопасности. Место информационной безопасности в национальной безопасности РФ

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»

Тема 2. Построение системы защиты информации в организации

Понятие угрозы. Защита. Классификация угроз и мер защиты информации. Таксономия нарушений ИБ вычислительной системы и причины, обуславливающие их существование. Состав и содержание средств защиты, объекты и элементы защиты. ГОСТ

34.603-92 «Информационная технология. Виды испытаний автоматизированных систем». ГОСТ Р 50922-2006 «Защита информации. Основные термины и определения». ГОСТ Р 51275-2006 «Защита информации. Объект информатизации. Факторы, воздействующие на информацию. Общие положения». ГОСТ Р 51583-2000 «Защита информации. Порядок создания автоматизированных систем в защищенном исполнении. Общие положения».

Тема 3. Современные методики анализа и управления рисками информационной безопасности

Классификация каналов проникновения в систему и утечки информации. Неформальная модель нарушителя в АС. Виды противников или «нарушителей». Анализ способов нарушений ИБ. Понятия о видах вирусов. ГОСТ Р 51624-2000 «Защита информации. Автоматизированные системы в защищенном исполнении. Общие требования». ГОСТ Р ИСО/МЭК 27002-2012 «Информационная технология. Методы и средства обеспечения безопасности. Свод норм и правил менеджмента информационной безопасности». ГОСТ Р ИСО/МЭК 29100-2013 «Информационная технология. Методы и средства обеспечения безопасности. Основы обеспечения приватности». ISO/IEC 27000:2009 – СУИБ: определения и основные принципы.

Тема 4. Основные программно-технические меры безопасности информации: идентификация и аутентификация; управление доступом

Основы безопасности жизнедеятельности в области профессиональной деятельности. Постановка и решение схемотехнические задачи, связанные с выбором системы эле-

ментов при заданных требованиях к параметрам (временным, мощностным, габаритным, надежностным. Принципы реализации и использования алгоритмов идентификации и аутентификации, управления доступом и процедур анализа защищенности.

Тема 5. Основные программно-технические меры безопасности информации: протоколирование, аудит, шифрование, контроль целостности, электронная подпись

Основные понятия. Описывается протоколирование и аудит, а также криптографические методы защиты. Показывается их место в общей архитектуре безопасности. Методы шифрования. Криптографического контроля целостности. Цифровые сертификаты.

Тема 6. Основные технологии построения защищенных систем

Основные технологии построения защищенных систем. Физические устройства. Их виды и использование. Программные пакеты. Виды программных пакетов для обеспечения защищенной системы. Правовые особенности использования средств информационной защиты.

5. ПЕРЕЧЕНЬ УЧЕБНО-МЕТОДИЧЕСКОГО ОБЕСПЕЧЕНИЯ ДЛЯ САМОСТОЯТЕЛЬНОЙ РАБОТЫ ОБУЧАЮЩИХСЯ

5.1. Указания по организации и проведению лекционных,) и лабораторных занятий с перечнем учебно-методического обеспечения

Для успешного освоения дисциплины является обязательным посещение всех занятий, выполнение домашнего задания и иных форм самостоятельной работы, которые назначаются преподавателем.

Особенность изучения дисциплины состоит из лекций с элементами беседы. Такие лекции эффективны тем, что предусматривают использование вопросно-ответной формы подачи материала, то есть преподаватель использует приемы скрытого диалога, когда лектор с помощью студентов отвечает на поставленные проблемные вопросы. А также выполнение комплекса лабораторных работ, главной задачей которых является получение навыков самостоятельной работы на компьютерах с использованием современных информационных систем и программного обеспечения для решения различных учебных и профессиональных задач.

Методическая поддержка дисциплины обеспечивается использованием дистанционных технологий. Студентам предлагается информационный ресурс, расположенный по адресу: http://moodle.asu.edu.ru, на сервере дистанционного обучения АГУ. Доступ студентов к учебным ресурсам осуществляется по учетной записи и паролю после регистрации на курс «Безопасность информационных систем и технологий» на период обучения по данной дисциплине.

На сервере размещен методический материал по данной дисциплине, в содержание которого входит:

- теоретический материал;
- мультимедийные презентации по тематикам лекций;
- задания и указания по выполнению лабораторно-практических работ, требования к содержанию и их оформлению, рекомендации по их защите;
- тестовые вопросы, предназначенные всех видов контроля, включая самоконтроль освоения учебного материала;
- вопросы к экзамену.

Аудиторные занятия проводятся на основе теоретического материала, опубликованного на образовательном портале, это позволяет студентам изучить пропущенный материал или самостоятельно разобраться с темой, не освоенной на занятии.

5.2. Указания для обучающихся по освоению дисциплины (модуля)

Лекция

- Лекция – основной вид обучения в вузе.
- В лекции излагаются основные положения теории, ее понятия и законы, приводятся факты, показывающие связь теории с практикой.

– Накануне лекции необходимо повторить содержание предыдущей лекции (а также теорию по изучаемой теме в школьных учебниках геометрии, если эта тема была представлена в них), а затем посмотреть тему очередной лекции по программе (по плану лекций).
– Полезно вести записи (конспекты) лекций: для непонятных вопросов оставлять место при работе над темой лекции с учебными пособиями.
– Записи лекций следует вести в отдельной тетради, оставляя место для дополнений во время самостоятельной работы.
– При конспектировании лекций выделяйте главы и разделы, параграфы, подчеркивайте основное.

Лабораторное занятие

Лабораторное занятие – наиболее активный вид учебных занятий в вузе. Он предполагает самостоятельную работу над лекциями и учебными пособиями.

К каждому лабораторному занятию нужно готовиться. Подготовку следует начинать с повторения теории (по записям лекций или по учебному пособию). После этого нужно решать задачи из предложенного домашнего задания.

Самостоятельная работа по освоению дисциплины включает:
– изучение дополнительной учебной литературы и посещение Интернет-ресурсов;
– работа с материалами лекций (обработка текста), самоконтроль изученного теоретического материала, подготовка к тестированию и промежуточной аттестации;

Планирование времени, необходимого на изучение дисциплин, студентам лучше всего осуществлять весь семестр, предусматривая при этом регулярное повторение материала.

При изучении дисциплины сначала необходимо по каждой теме прочитать рекомендованную литературу и составить краткий конспект основных положений, терминов, сведений, требующих запоминания и являющихся основополагающими в этой теме для освоения последующих тем курса. Для расширения знания по дисциплине рекомендуется использовать Интернет-ресурсы; проводить поиски в различных системах и использовать материалы сайтов, рекомендованных преподавателем.

Таблица 4.
Содержание самостоятельной работы обучающихся

Номер раздела (темы)	Темы/вопросы, выносимые на самостоятельное изучение	Кол-во часов	Формы работы
1	Тема 1. Цели и задачи информационной безопасности. Место информационной безопасности в национальной безопасности РФ	9	Изучение учебной литературы и материалов лекций, самоконтроль
2	Тема 2. Построение системы защиты информации в организации	9	Изучение учебной литературы и материалов лекций, подготовка к тесту, самоконтроль
3	Тема 3. Современные методики анализа и управления рисками информационной безопасности	9	Изучение учебной литературы и материалов лекций, самоконтроль
4	Тема 4. Основные программно-технические меры безопасности информации: идентификация и аутентификация; управление доступом	9	Изучение учебной литературы и материалов лекций, подготовка к контрольной работе, самоконтроль
5	Тема 5. Основные программно-технические меры безопасности информации: протоколирование, аудит, шифрование, контроль целостности, электронная подпись	9	Изучение учебной литературы и материалов лекций, самоконтроль
6	Тема 6. Основные технологии построения защищенных систем	9	Изучение учебной литературы и материалов лекций, подготовка к контрольной работе, самоконтроль

5.3. Виды и формы письменных работ, предусмотренных при освоении дисциплины, выполняемые обучающимися самостоятельно:

Одним из видов письменных работ является самостоятельное подготовка отчетов по выполненным лабораторным работам. Отчет оформляется с помощью любого текстового редактора и должен содержать: описание процесса выполнения работы с предоставлением промежуточных и итоговых результатов. Результаты должны быть представлены, как в текстовом, так и в графическом виде.

6. ОБРАЗОВАТЕЛЬНЫЕ И ИНФОРМАЦИОННЫЕ ТЕХНОЛОГИИ

6.1. Образовательные технологии

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

При реализации различных видов учебной и внеучебной работы используются следующие информационные технологии:

- система управления обучением LMS Moodle;
- использование возможностей Интернета в учебном процессе (рассылка заданий, предоставление выполненных работ, ответы на вопросы, ознакомление обучающихся с оценками и т.д.);
- использование электронных учебников и различных сайтов (например, электронные библиотеки, журналы и т.д.) как источник информации;
- использование возможностей электронной почты;
- использование средств представления учебной информации (электронных учебных пособий, применение новых технологий для проведения занятий с использованием презентаций и т.д.);
- использование интерактивных средств взаимодействия участников образовательного процесса (технологии дистанционного или открытого обучения в глобальной сети);
- 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).

6.3. Перечень программного обеспечения и информационных справочных систем

Перечень программного обеспечения:

Наименование программного обеспечения	Назначение
Adobe Reader	Программа для просмотра электронных документов
Платформа дистанционного обучения LMS Moodle	Виртуальная обучающая среда
Microsoft Office 2013, Microsoft Office Project 2013, Microsoft Office Visio 2013	Пакет офисных программ
7-zip	Архиватор
Microsoft Windows 7 Professional	Операционная система
Google Chrome	Браузер
CodeBlocks	Кроссплатформенная среда разработки
Notepad++	Текстовый редактор
R	Программная среда вычислений
WinDjView	Программа для просмотра файлов в формате DJV и DjVu
Microsoft Visual Studio	Среда разработки

Перечень информационных справочных систем:

1. Электронная библиотека «Астраханский государственный университет» собственной генерации на платформе ЭБС «Электронный Читальный зал – БиблиоТех». https://biblio.asu.edu.ru
2. Электронно-библиотечная система (ЭБС) ООО «Политехресурс» «Консультант студента». www.studentlibrary.ru
3. Электронная библиотечная система издательства ЮРАЙТ, раздел «Легендарные книги». www.biblio-online.ru, https://urait.ru/
4. Электронная библиотечная система IPRbooks. www.iprbookshop.ru
5. Электронно-библиотечная система elibrary. http://elibrary.ru
6. Справочная правовая система КонсультантПлюс: http://www.consultant.ru
7. Информационно-правовое обеспечение «Система ГАРАНТ»: http://garant-astrakhan.ru

7. ФОНД ОЦЕНОЧНЫХ СРЕДСТВ ДЛЯ ТЕКУЩЕГО КОНТРОЛЯ И ПРОМЕЖУТОЧНОЙ АТТЕСТАЦИИ ПО ДИСЦИПЛИНЕ

7.1. Паспорт фонда оценочных средств

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

Таблица 5.
Соответствие изучаемых разделов, результатов обучения и оценочных средств

№ п/п	Контролируемые разделы дисциплины (модуля)	Код контролируемой компетенции (компетенций)	Наименование оценочного средства
1.	Тема 1. Цели и задачи информационной безопасности. Место информационной безопасности в национальной безопасности РФ	ПК 8	Лабораторная работа №1, устный опрос
2.	Тема 2. Построение системы защиты информации в организации	ПК 8	Тест, устный опрос
3.	Тема 3. Современные методики анализаи управления рисками информационной безопасности	ПК 8	Лабораторная работа №2, устный опрос
4.	Тема 4. Основные программно-технические меры безопасности информации: идентификация и аутентификация; управление доступом	ПК 8	Контрольная работа №1, Лабораторная работа №3
5.	Тема 5. Основные программно- технические меры безопасности информации: протоколирование, аудит, шифрование, контроль целостности, электронная подпись	ПК 8	Лабораторная работа №4, устный опрос
6.	Тема 6. Основные технологии построения защищенных систем	ПК 8	Контрольная работа №2, Лабораторная работа №5, устный опрос

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

Таблица 6.
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 «удовлетвори тельно»	демонстрирует неполное, фрагментарное знание теоретического материала, требующее наводящих вопросов преподавателя, допускает существенные ошибки в его изложении, затрудняется в приведении примеров и формулировке выводов
2 «неудовлетво рительно»	демонстрирует существенные пробелы в знании теоретического материала, не способен его изложить и ответить на наводящие вопросы преподавателя, не может привести примеры

Таблица7.
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 оценки знаний, умений, навыков и (или) опыта деятельности

В рабочей программе приведены фрагменты практических заданий. Полнотекстовые задания представлены на образовательном портале вуза.

Тема 1. Цели и задачи информационной безопасности. Место информационной безопасности в национальной безопасности РФ

Лабораторная работа 1.

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:

- организационные;

- технологические;
- 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:

- индивидуального объекта заданного типа;
- знаний некоторой известной только ему и проверяющей стороне информации;
- 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.

В 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:

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.

Задания.

1. 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

Тема 2. Построение системы защиты информации в организации

Тест

Банк тестовых заданий размещен на сайте центра цифрового обучения http://moodle.asu.edu.ru

1. По объекту воздействия угрозы бывают:
   - воздействующие на информационную среду в целом
   - воздействующие на отдельные элементы информационной среды
   - активные
   - пассивные
2. Выберите правильный вариант ответа. Событие, являющееся следствием одного или нескольких нежелательных или неожиданных событий (информационной безопасности), имеющих значительную вероятность компрометации бизнесопераций и создания угрозы
   - инцидент
   - нарушение
   - сигнал

3. Идентифицированное появление определенного состояния системы, сервиса или сети, указывающего на возможное нарушение политики информационной безопасности, или отказ защитных мер, или возникновение неизвестной ранее ситуации, которая может иметь отношение к безопасности называется
   - событием (информационной безопасности)
   - инцидентом (информационной безопасности) угрозой (информационной безопасности)
4. Первым шагом в управлении сетью является ее
   - документирование
   - ревизия
   - оформление
5. Какова цель ревизии эффективности?
   - Мониторинг и анализ работы сети.
   - Определение того, работает ли сеть в соответствии со своим потенциалом.
   - Идентификация типов оборудования и устройств, сети.
   - Обеспечение информации о восстановлении после сбоя или катастрофического отказа.

Тема 3. Современные методики анализа и управления рисками информационной безопасности

Лабораторная работа 2. Архивирование с паролем

Необходимо создать текстовый файл, содержащий фамилию, имя, отчество студента в объеме 50 записей. Провести архивирование файла. Любым редактором внести изменения согласно задания. В отчете отразить: контрольную сумму исходного файла, сжатого файла, выдаваемые сообщения об ошибках при разархивировании искаженного файла.

Провести архивацию файла с паролем. Внести искажения, попробовать разархивировать. В отчете отразить: контрольную сумму исходного файла, сжатого файла, выдаваемые сообщения об ошибках при разархивировании искаженного файла.

Провести архивацию файла с паролем, состоящим из 3-х цифр. Провести попытку подбора пароля с использованием программного обеспечения. В отчете отразить: контрольную сумму исходного файла, сжатого файла, выдаваемые сообщения, время подбора.

Варианты:

архиватор zip. Искажение двух байт. архиватор arj. Искажение трех байт. архиватор rar. Искажение трех байт. архиватор zip. Удаление двух байт. архиватор arj. Удаление трех байт. архиватор rar. Удаление трех байт. архиватор arj. Добавление трех байт. архиватор rar. Добавление трех байт. архиватор zip. Добавление двух байт. архиватор zip. Удаление двух байт.

Тема 4. Основные программно-технические меры безопасности информации: идентификация и аутентификация; управление доступом

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. Компьютеные «Вирусы». Их виды
11. Способы борьбы с компьютерными вирусами

Лабораторная работа 3.

Цель работы: реализовать в «командном процессоре» защиту на уровне пользователя с

применением метода паролей или его модификаций; реализовать процедуру управления системой защиты на уровне пользователя

Структура командного процессора (блок «защита на уровне пользователя»)

Субъекты: Суперпользователь/администратор, другие пользователи

Объекты: база учетных записей пользователей

Минимальный набор команд:

изменение своего пароля, добавление нового пользователя, удаление пользователя, изменение учетной записи пользователя (изменение логина, дополнительных полей учетной записи (если они есть)), просмотр информации о текущем пользователе, просмотр разрешенной информации о существующих в системе пользователях, несколько нейтральных команд (дата, время, список доступных команд системы и

т.п.).

Минимальная функциональность:

пароль не должен быть виден на экране, в системе всегда присутствует хотя бы один суперпользователь, обыкновенный пользователь ограничен в действиях, создаёт новых пользователей (удаляет существующих) только суперпользователь, суперпользователь может изменять пароли всех пользователей, при изменении/добавлении пароля запрашивается его подтверждение, имена пользователей в системе попарно различны (не повторяются), возможность зайти под другим пользователем, не закрывая приложение, работать в системе может только пользователь, успешно прошедший процедуру аутентификации

Тема 5. Основные программно-технические меры безопасности информации: протоколирование, аудит, шифрование, контроль целостности, электронная подпись

Лабораторная работа 4.

Реализовать приложение, позволяющие решить задачи в соответствии с вариантом.

Задачи

1. Для указанных открытых ключей пользователя RSA проверить подлинность подписанных сообщений:

1) n=55, e=3: <7,28>, <22,15>,<16,36>
2) n=65, e=5: <6,42>, <10,30>,<6,41>
3) n=77, e=7: <13,41>, <11,28>,<5,26>
4) n=91, e=5: <15,71>, <11,46>,<16,74>
5) n=33, e=3: <10,14>, <24,18>,<17,8>

2. Абоненты некоторой сети применяют подпись Эль-Гамаля с общими параметрами p=23, g=5. Для указанных секретных параметров абонентов найти открытый ключ (y) и построить подпись для сообщения m:

1) x=11, k=3, m=15
2) x=10, k=15, m=5
3) x=3, k=13, m=8
4) x=18, k=7, m=5
5) x=9, k=19, m=15

Во всех вариантах будем предполагать, что h(m)=m для всех значений m.

№ варианта	№ задач
1	1.1 , 2.1
2	1.2 , 2.2
3	1.3 , 2.3
4	1.4 , 2.4

5	1.5 , 2.5
6	1.4 , 2.2
7	1.3 , 2.1

Тема 6. Основные технологии построения защищенных систем

Лабораторная работа 5.

Цель работы: изучение принципов защиты ресурсов с помощью управления доступом и приобретение навыков администрирования системы защиты информации Secret Net 7.

Задача №1: Изучить теоретический материал по работе с системой защиты компьютера от несанкционированного доступа: Secret Net 7.

Задача №2: управление доступом и защита ресурсов в системе Secret Net 7.

Контрольная работа № 2

1. Определение понятия «Система информационной безопасности»
2. Элементы системы информационной безопасности
3. Определение понятия «Государственная тайна»
4. Регулирование правовых отношений в области защиты государственной тайны
5. Модели безопасности их применение
6. Место ИБ экономических систем в национальной безопасности страны
7. Основы конфиденциального документооборота
8. Особенности работы с персоналом, владеющим конфиденциальной информацией
9. Принципы построения защищенных компьютерных систем
10. Элементы операционной системы
11. Управление доступом пользователей в опреационных системах
12. Парольная политика популярных операционных систем
13. Состав локально-вычислительных сетей
14. Коммутаторы, концентраторы, маршрутизаторы
15. Организация доступа в локальных сетях
16. Контроль сетевых подключений
17. Управление сетевой маршрутизацией
18. Управление доступом к компьютерам
19. Система управления паролями
20. Управление доступом к приложениям
21. Управление доступом к библиотекам исходных текстов программ

Примерный 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 нарушите-

лей 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.

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

Оценка качества освоения дисциплины в ходе текущей и промежуточной аттестации обучающихся осуществляется в соответствии с «Положением о балльно-рейтинговой системе оценки учебных достижений студентов» (приказ от 13.01.2014 № 08-01-01/08).

Преподаватель, реализующий дисциплину, в зависимости от уровня подготовленности обучающихся может использовать иные формы, методы контроля и оценочные средства, исходя из конкретной ситуации.

8. УЧЕБНО-МЕТОДИЧЕСКОЕ И ИНФОРМАЦИОННОЕ ОБЕСПЕЧЕНИЕ ДИСЦИПЛИНЫ

а) 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»).

б) дополнительная литература

1. Основы информационной безопасности: 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»).
2. Информационная безопасность: защита и нападение / Бирюков А.А. - М.: ДМК Пресс, 2012. - URL: http://www.studentlibrary.ru/book/ISBN9785940746478.html (ЭБС «Консультант студента»).
3. Основы информационной безопасности : учебное пособие для студентов вузов / Е.В. Вострецова.— Екатеринбург : Изд-во Урал. ун-та, 2019.— 204 с
4. 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 с.
5. Хорев П.Б. Методы и средства защиты информации в компьютерных системах: уч.пособие. – М.: Издат центр «Академия», 2005, – 256 с. 7. 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.

в) Перечень ресурсов информационно-телекоммуникационной сети «Интернет», необходимый для освоения дисциплины

1. Электронный каталог Научной библиотеки АГУ на базе MARK SQL НПО «Информ-систем»: https://library.asu.edu.ru
2. Корпоративный проект Ассоциации региональных библиотечных консорциумов (АРБИКОН) «Межрегиональная аналитическая роспись статей» (МАРС): http://mars.arbicon.ru
3. Единое окно доступа к образовательным ресурсам http://window.edu.ru

9. МАТЕРИАЛЬНО-ТЕХНИЧЕСКОЕ ОБЕСПЕЧЕНИЕ ДИСЦИПЛИНЫ

Лекционные занятия проводятся в аудиториях, оснащенных мультимедийным оборудованием: проектор и экран проектора. Лабораторные работы проводятся в дисплейных классах, оснащенных программным обеспечением, указанным в пункте 6.3 и доступом в Интернет. Для самостоятельной работы в распоряжении студента имеются читальный зал и дисплейные классы, обеспечивающие свободный доступ в Интернет.

При необходимости рабочая программа дисциплины (модуля) может быть адаптирована для обеспечения образовательного процесса инвалидов и лиц с ограниченными возможностями здоровья, в том числе для обучения с применением дистанционных образовательных технологий. Для этого требуется заявление студента (его законного представителя) и заключение психолого-медико-педагогической комиссии (ПМПК).