

Государственное профессиональное образовательное учреждение Тульской области «Донской политехнический колледж»
Задания для выполнения самостоятельной работы

студентами отделения 10.02.05 Обеспечение информационной безопасности автоматизированных систем
по *МДК 02.01* Программные и программно-аппаратные средства защиты информации

ПОЯСНИТЕЛЬНАЯ ЗАПИСКА

Основное назначение МДК.02.01 Программные и программно-аппаратные средства защиты информации в средних профессиональных образовательных организациях состоит в формировании у студентов общих и профессиональных компетенций: выбирать способы решения задач профессиональной деятельности, применительно к различным контекстам; осуществлять поиск, анализ и интерпретацию информации, необходимой для выполнения задач профессиональной деятельности; планировать и реализовывать собственное профессиональное и личностное развитие; работать в коллективе и команде, эффективно взаимодействовать с коллегами, руководством, клиентами; осуществлять устную и письменную коммуникацию на государственном языке с учетом особенностей социального и культурного контекста; проявлять гражданско-патриотическую позицию, демонстрировать осознанное поведение на основе традиционных общечеловеческих ценностей; содействовать сохранению окружающей среды, ресурсосбережению, эффективно действовать в чрезвычайных ситуациях; использовать средства физической культуры для сохранения и укрепления здоровья в процессе профессиональной деятельности и поддержания необходимого уровня физической подготовленности; использовать информационные технологии в профессиональной деятельности; пользоваться профессиональной документацией на государственном и иностранном языках;

осуществлять установку и настройку отдельных программных, программно-аппаратных средств защиты информации; обеспечивать защиту информации в автоматизированных системах отдельными программными, программно-аппаратными средствами; осуществлять тестирование функций отдельных программных и программно-аппаратных средств защиты информации; осуществлять обработку, хранение и передачу информации ограниченного доступа; уничтожать информацию и носители информации с использованием программных и программно-аппаратных средств; осуществлять регистрацию основных событий в автоматизированных (информационных) системах, в том числе с использованием программных и программно-аппаратных средств обнаружения, предупреждения и ликвидации последствий компьютерных атак.

Практическое занятие – это форма организации учебного процесса, предполагающая выполнение обучающимися заданий самостоятельно и под руководством преподавателя. Дидактическая цель практических работ – формирование у обучающихся профессиональных и практических умений, необходимых для изучения последующих учебных дисциплин, а также подготовка к применению этих умений в профессиональной деятельности.

Практические занятия предполагают работу по обнаружению угроз безопасности информации, защите информации, информационных систем, компьютерных сетей.

Осуществлять регистрацию основных событий в автоматизированных (информационных) системах, в том числе с использованием программных и программно-аппаратных средств обнаружения, предупреждения и ликвидации последствий компьютерных атак.

Разработано содержание, определена их цель, даны методические указания по выполнению заданий и упражнений, указана учебная и справочная литература. Структура рекомендаций соответствует структуре междисциплинарного курса Программные и программно-аппаратные средства защиты информации.

ПРАВИЛА ВЫПОЛНЕНИЯ ПРАКТИЧЕСКИХ РАБОТ

В ходе выполнения практических работ студент должен:

- ✓ выполнять требования по охране труда

- ✓ соблюдать инструкцию по правилам и мерам безопасности в лаборатории информационных технологий
- ✓ строго выполнять весь объем работы, указанный в задании
- ✓ соблюдать требования эксплуатации компьютерной техники (правила включения и выключения)
- ✓ изучить теоретические вопросы, используя лекционный материал к теме
- ✓ предоставить отчет о проделанной работе по окончании выполненной работы.

РЕКОМЕНДАЦИИ ПО ОФОРМЛЕНИЮ ПРАКТИЧЕСКОЙ РАБОТЫ

- ✓ при выполнении практической работы в программе MS Word необходимо выбирать гарнитуру и размер шрифтов, выравнивание, отступы и интервалы в соответствии с заданием;
- ✓ при выполнении в программе MS Word практической работы содержащей таблицы соблюдать структуру и выравнивание ячеек таблиц, цвет границы и заливки фигур;
- ✓ при выполнении практической работы в программе MS Excel соблюдать формат и выравнивание ячеек, название листов, точность вычислений в соответствии с заданием.
- ✓ при выполнении практической работы в программе MS Power Point необходимо выбирать гарнитуру и размер шрифтов, выравнивание, отступы и интервалы, макеты оформления, графические объекты, анимацию и переходы в соответствии с заданием;
- ✓ при выполнении практической работы в программе MS Access (создание базы) в таблицы добавлять не менее 10 записей, таблицы переименовывать в соответствии с заданием, отчеты формировать в табличной форме, кнопочная форма обязательна.

Работы проводятся согласно календарно-тематическому планированию, в соответствии с учебной программой. Пропущенные практические работы

выполняются обучающимися самостоятельно и сдаются в отведенные на изучение дисциплины сроки.

КРИТЕРИИ ОЦЕНИВАНИЯ

Оценка «Отлично» - полно раскрыто содержание материала в объеме, предусмотренном программой, практическая работа выполнена правильно, в полном объеме и защищена.

«Хорошо» - в изложении материала допущены небольшие пробелы, не исказившие логического и информационного содержания ответа; допущены один-два недочета при освещении основного содержания ответа, исправленные по замечанию преподавателя; в выполненной практической работе допущены в ответах отдельные неточности, исправленные с помощью преподавателя.

«Удовлетворительно» - неполно или непоследовательно раскрыто содержание материала, но показано общее понимание вопроса и продемонстрированы умения, достаточные для дальнейшего усвоения программного материала, имелись затруднения или допущены ошибки в определении понятий, использовании терминологии; практическая работа выполнена частично, допущены ошибки и неточности, которые не всегда исправляются с помощью преподавателя.

«Неудовлетворительно» - не раскрыто основное содержание учебного материала; обнаружено незнание или непонимание обучающимся большей или наиболее важной части учебного материала; практическая работа носит трафаретный характер, выполнена неправильно или не выполнена вовсе.

ПЕРЕЧЕНЬ ПРАКТИЧЕСКИХ ЗАНЯТИЙ

Номер темы	Номер и наименование работы (занятия)	Кол-во ауд-х часов	
1	2	3	
1.2	Практическое занятие № 1. Обзор нормативных правовых актов, нормативных методических	2	ПК 2.1 - ПК 2.6

	документов по защите информации, в состав которых входят требования и рекомендации по защите информации программными и программно-аппаратными средствами. Работа с содержанием нормативных правовых актов.		
	Практическое занятие № 2. Обзор стандартов. Работа с содержанием стандартов	2	
1.3	Практическое занятие № 3. Учет, обработка, хранение и передача информации в АИС	2	ПК 2.1 - ПК 2.6
	Практическое занятие № 4. Ограничение доступа на вход в систему.	2	
	Практическое занятие № 5. Идентификация и аутентификация пользователей	2	
	Практическое занятие № 6. Разграничение доступа.	2	

ПРАКТИЧЕСКОЕ ЗАНЯТИЕ № 1.

ОБЗОР НОРМАТИВНЫХ ПРАВОВЫХ АКТОВ, НОРМАТИВНЫХ МЕТОДИЧЕСКИХ ДОКУМЕНТОВ ПО ЗАЩИТЕ ИНФОРМАЦИИ, В СОСТАВ КОТОРЫХ ВХОДЯТ ТРЕБОВАНИЯ И РЕКОМЕНДАЦИИ ПО ЗАЩИТЕ ИНФОРМАЦИИ ПРОГРАММНЫМИ И ПРОГРАММНО-АППАРАТНЫМИ СРЕДСТВАМИ. РАБОТА С СОДЕРЖАНИЕМ НОРМАТИВНЫХ ПРАВОВЫХ АКТОВ

Цель: научиться работать в справочно-правовой системе с нормативными и правовыми документами по защите информации.

Теоретические вопросы

1. Предмет и задачи программно-аппаратной защиты информации.
2. Основные понятия программно-аппаратной защиты информации.
3. Классификация методов и средств программно-аппаратной защиты информации.

4. Нормативные правовые акты, нормативные методические документы, в состав которых входят требования и рекомендации по защите информации программными и программноаппаратными средствами.

Приложение перечень основных нормативных документов, регламентирующих деятельность области защиты информации:

– Конституция Российской Федерации;

– Гражданский Кодекс Российской Федерации

– Уголовный Кодекс Российской Федерации

– Доктрина информационной безопасности Российской Федерации; – Законы Российской Федерации:

Федеральный закон РФ от 21.07.1993 № 5485-1 «О государственной тайне»;

Федеральный закон РФ от 27.06.2006 № 149-ФЗ «Об информации, информационных технологиях и защите информации»;

Федеральный закон РФ от 27.07.2006 № 152-ФЗ «О персональных данных»;

Федеральный закон РФ от 06.04.2011 № 63-ФЗ «Об электронной подписи»;
Федеральный закон от 29.04.2004 № 98-ФЗ «О коммерческой тайне»; – Указы Президента Российской Федерации:

Указ Президента РФ от 30 ноября 1995 г. №1203 «Об утверждении перечня сведений, отнесенных к государственной тайне»;

Указ Президента РФ от 6 марта 1997 г. №188 «Об утверждении перечня сведений конфиденциального характера»;

– Постановления Правительства Российской Федерации:

Постановление Правительства РФ от 01.11.2012 №1119 «Об утверждении требований к защите персональных данных при их обработке в информационных системах персональных данных»;

Постановление Правительства РФ от 03.02.2012 № 79 "О лицензировании деятельности по технической защите конфиденциальной информации"; – Документы ФСТЭК, ФСБ:

Приказ от 11 февраля 2013г. № 17 «Об утверждении требований о защите информации, не составляющей государственную тайну, содержащейся в государственных информационных системах»;

Приказ ФСТЭК России от 18.02.2013 № 21 «Об утверждении состава и содержания организационных и технических мер по обеспечению безопасности персональных данных при их обработке в информационных системах персональных данных»; руководящие документы ФСТЭК по защите от НСД; руководящие документы ФСТЭК по защите от НДВ;

Положение по аттестации объектов информатизации по требованиям безопасности информации от 25 ноября 1994 г.;

Специальные требования и рекомендации по технической защите конфиденциальной информации (СТР-К);

Приказ ФСБ РФ от 9 февраля 2005г. № 66 «Об утверждении, разработке, производстве, реализации и эксплуатации шифровальных и криптографических средств защиты (Положение ПКЗ-2005)».

Задание 1. Определить нормативные методические документы, в состав которых входят требования и рекомендации по защите информации программными и программно-аппаратными средствами.

Задание 2. Изучить ФЗ «Об информации, информационных технологиях и о защите информации». Выписать требования и рекомендации по защите информации программными и программно-аппаратными средствами.

Задание 3. Изучить приказ ФСТЭК России от 18 февраля 2013 г.; 21 «Об утверждении состава и содержания организационных и технических мер по обеспечению безопасности персональных данных при их обработке в информационных системах персональных данных». Выписать требования и рекомендации по защите информации программными и программно-аппаратными средствами.

Задание 4. Изучить типовые требования по организации и обеспечению функционирования шифровальных (криптографических) средств, предназначенных для защиты информации, не содержащей сведений, составляющих государственную тайну в случае их использования для обеспечения безопасности персональных данных при их обработке в информационных системах персональных данных, утвержденные руководством Центра ФСБ России 21.02.2008 №149/6/6622.

Выписать требования и рекомендации по защите информации программными и программноаппаратными средствами.

ПРАКТИЧЕСКОЕ ЗАНЯТИЕ № 2.

ОБЗОР СТАНДАРТОВ. РАБОТА С СОДЕРЖАНИЕМ СТАНДАРТОВ

Цели: научиться работать в справочно-правовой системе с нормативными и правовыми документами по защите информации.

Теоретические вопросы

1. Предмет и задачи программно-аппаратной защиты информации.
2. Основные понятия программно-аппаратной защиты информации.
3. Классификация методов и средств программно-аппаратной защиты информации.
4. Стандарты по защите информации, в состав которых входят требования и рекомендации по защите информации программными и программно-аппаратными средствами.

Задание 1. Выписать государственные стандарты в области информационной безопасности.

Задание 2. Выписать международные стандарты информационной безопасности.

Задание 3. Изучить ГОСТ Р ИСО/МЭК 17799-2005 «Информационная технология. Практические правила управления информационной безопасностью». Выписать требования и рекомендации по защите информации программными и программно-аппаратными средствами.

ПРАКТИЧЕСКОЕ ЗАНЯТИЕ № 3.

УЧЕТ, ОБРАБОТКА, ХРАНЕНИЕ И ПЕРЕДАЧА ИНФОРМАЦИИ В АИС

Цели: познакомиться со способами учета, обработки, хранения и передачи информации в АИС.

Теоретические вопросы

1. Технологии учета и хранения информации.

2. Технологический процесс обработки информации.
3. Способы обработки информации.
4. Режимы обработки информации на компьютере.
5. Технологии передачи и представления информации.

Задание 1. Изучить технологии учета и хранения информации. Описать, как происходит сбор и регистрация данных. Назовите основные требования к сбору данных и к хранимым данным. Перечислите основные средства сбора текстовой, графической, звуковой и видеоинформации. Какие еще средства сбора информации вам известны?

Задание 2. Изучить технологический процесс обработки информации. Перечислить и охарактеризовать технологические процессы процесса обработки информации. В чем заключается различие между централизованным и децентрализованным способами обработки информации? Какие режимы обработки информации вам известны?

Задание 3. Изучить технологии передачи и представления информации. Описать, как происходит передача данных. **Задание 4.** Выполнить задания:

набрать в одном из текстовых редакторов текст из 10 предложений на тему «Моя профессия»; вставить в набранный текст рисунок; сохранить текст на каких-либо носителях; создать свою электронную почту; отправить, набранную информацию по электронной почте; получить информацию по электронной почте; изменить полученный текст, введя диаграмму; сохранить текст.

Задание 5. Продумать и создать технологию учета и отработки заявок на выполнение работ по ремонту компьютерной техники в салоне по ремонту компьютерного оборудования «СервисТЕХНО». Результат выполнения задания оформить в виде таблицы.

Задание 6. Используя технологии поиска информации, найдите разницу между терминами “хранение” и “сохранение данных”.

Задание 7. Используя средства Интернета, перечислите устройства защиты технических устройств информатизации от изменения напряжения и тока их электропитания.

ПРАКТИЧЕСКОЕ ЗАНЯТИЕ № 4.

ОГРАНИЧЕНИЕ ДОСТУПА НА ВХОД В СИСТЕМУ

Цель: ознакомиться с процедурами создания учётных записей пользователей и управления их правами.

Теоретические вопросы

1. Учётные записи пользователей.
2. Создание учётных записей пользователей.
3. Создание учётных записей пользователей для компьютеров, состоящих в рабочей группе.
4. Создание учётной записи при помощи оснастки «Локальные пользователи и группы».
5. Создание учётной записи при помощи командной строки.
6. Управление учётными записями при помощи диалога «Управление учётными записями пользователей».

Задание 1. Ознакомиться с технологиями создания и управления учётными записями пользователей. Примените к созданной учётной записи настройки, указанные в варианте.

Таблица 1 – Варианты заданий

Параметр \ Вариант	1	2	3	4	5	6	7	8	9	10
Максимальный срок действия пароля	30	90	60	30	90	60	30	90	60	30
Минимальная длина пароля	6	7	8	9	10	6	7	8	9	10
Требовать неповторяемости паролей	6	5	4	3	2	6	5	4	3	2
Пароль должен отвечать требованиям сложности	+	-	-	+	-	-	+	-	+	+
Пороговое значение блокировки	3	4	5	6	7	3	4	5	6	7
Блокировка учётной записи на...	10	20	30	45	60	10	20	30	45	60
Сброс счётчика блокировки через...	5	10	15	20	30	10	20	30	45	60
Завершение работы системы	+	+			+		+		+	
Локальный вход в систему	+	+	+	+	+	+	+	+	+	+
Изменение системного времени	+		+		+		+		+	

Задание 2. Создайте новую учетную запись пользователя с помощью командной строки.

Задание 3. Создайте учетные записи для двух разных пользователей. Для одного пользователя проверьте действенность флажка – требования смены пароля пользователя при следующей регистрации в системе, для другого – запрет на изменение пароля пользователем.

Задание 4. Создайте локальную группу. Поместите в локальную группу созданных вами пользователей и административного пользователя. Прделайте это двумя способами: через окно свойств группы и окно свойств пользователя.

ПРАКТИЧЕСКОЕ ЗАНЯТИЕ № 5.

ИДЕНТИФИКАЦИЯ И АУТЕНТИФИКАЦИЯ ПОЛЬЗОВАТЕЛЕЙ

Цель: ознакомиться с механизмами идентификации и аутентификации пользователей.

Теоретические вопросы

1. Понятия идентификации и аутентификации пользователей.
2. Механизмы аутентификации и идентификации пользователей.

Задание 1. Опишите параметры локальной политики безопасности операционной системы Windows:

- кто имеет доступ к компьютеру;
- какие ресурсы могут использовать пользователи на компьютере;
- включение и выключение записи действий пользователей или группы пользователей в журнале событий.

Задание 2. Опишите параметры и значения параметров Политики паролей. Заполните таблицу:

Параметр	Значение
Требовать повторяемости паролей	
Максимальный срок действия пароля	
Минимальный срок действия пароля.	
Минимальная длина пароля.	
Пароль должен отвечать требованиям сложности	
Хранить пароли всех пользователей в домене, используя обратимое шифрование.	

Задание 3. Опишите параметры и значения параметров Политики учетной записи. Заполните таблицу:

Параметр	Значение
Пороговое значение блокировки	
Блокировка учетной записи на	
Сброс счетчика блокировки через	

Задание 4. Измените параметр «Пароль должен отвечать требованиям сложности» Политики паролей на «Включен» и после этого попробуйте изменить пароль своей учетной записи. Зафиксируйте все сообщения системы, проанализируйте и введите допустимый пароль. Этот пароль является результатом выполнения вашего задания.

Задание 5. После успешного выполнения предыдущего задания, измените пароль вашей учетной записи, а в качестве нового пароля укажите прежний пароль. Все сообщения зафиксируйте, проанализируйте и объясните поведение системы безопасности.

Задание 6. Проведите эксперименты с другими параметрами Политики учетных записей.

Источники

1. Белов Е. Б. Организационно-правовое обеспечение информационной безопасности: учеб. пособие для студ. учреждений сред. проф. образования – М.: Издательский центр «Академия», 2017 – 336 с.

2. Баранова, Е. К. Информационная безопасность. История специальных методов криптографической деятельности: Учебное пособие / Баранова Е.К., Бабаш А.В., Ларин Д.А. - Москва: ИЦ РИОР, НИЦ ИНФРА-М, 2019. [Электронный ресурс; Режим доступа <http://znanium.com>]

3. Организационное и правовое обеспечение информационной безопасности: учебник и практикум для среднего профессионального образования / Т. А. Полякова, А. А. Стрельцов, С. Г. Чубукова, В. А. Ниесов ; ответственный редактор Т. А. Полякова, А. А. Стрельцов. — Москва: Издательство Юрайт, 2019. — 325 с. — (Профессиональное образование). [Электронный ресурс; Режим доступа <https://www.biblio-online.ru>]

Электронные ресурсы:

1. Федеральная служба по техническому и экспортному контролю (ФСТЭК России) www.fstec.ru

2. Информационно-справочная система по документам в области технической защиты информации www.fstec.ru

3. Образовательные порталы по различным направлениям образования и тематике <http://depobr.gov35.ru>

4. Справочно-правовая система «Консультант Плюс» www.consultant.ru
Справочно-правовая система «Гарант» www.garant.ru

5. Сайт Научной электронной библиотеки www.elibrary.ru