Информация для размещения на официальном сайте ГБПОУ «Светлоградский региональный сельскохозяйственный колледж»

Для электронного обучения

Группа	321
Дата	04.05.2021г
Время	15-00-16-20
Наименование УД/МДК/УП/ПП	МДК 02.01
Ф.И.О. преподавателя	Сахарчук Т.В.
Электронная почта	saharchyk777@mail.ru
Основная литература	1. Федорова Г.Н. Разработка и администрирование баз данных (2-е изд., стер.) учебник«Академия»2020 г. 2. Федорова Г.Н. Информационные системы (6-е изд., стер.) учебник «Академия» 2018г 3. Рудаков А.В. Технология разработки программных продуктов (12-е изд.) учебник«Академия»2018 г. 4. Фёдорова Г.Н. Основы проектирования баз данных (2-е изд., стер.) учебник «Академия»2018г. 5. Основы проектирования приложений баз данных Баженова И.Ю. Интуит НОУ 2016 https://www.book.ru/book/917912 6. Базы данных. (СПО). Учебник Кумскова И.А. КноРус 2019 https://www.book.ru/book/932018
Тема № 117-118	Практическое занятие на тему: Защита информации
Задание	Теоретическое обоснование работы: Информационная безопасность Информационная безопасность государства – состояние сохранности информационных ресурсов государства и защищённости законных прав личности и общества в информационной сфере. Информационная безопасность - это процесс обеспечения конфиденциальности, целостности и доступности информации. Конфиденциальность: Обеспечение доступа к информации только авторизованным пользователям. Целостность: Обеспечение достоверности и полноты информации и методов ее обработки. Доступность: Обеспечение доступа к информации и связанным с ней активам авторизованных пользователей по мере необходимости. Информационная безопасность – все аспекты, связанные с определением, достижением и поддержанием конфиденциальности, целостности, доступности, неотказуемости, подотчётности, аутентичности и достоверности информации или средств её обработки. Безопасность информации (данных) – состояние защищённости информации (данных), при котором обеспечиваются её (их) конфиденциальность, доступность и целостность. Безопасность информации (данных) определяется отсутствием недопустимого риска, связанного с утечкой информации по

	техническим каналам, несанкционированными и непреднамеренными воздействиями на данные и (или) на другие ресурсы автоматизированной информационной системы, используемые в автоматизированной системе. Вирусы. Антивирусное программное обеспечение Компьютерный вирус - программа способная самопроизвольно внедряться и внедрять свои копии в другие программы, файлы, системные области компьютера и в вычислительные сети, с целью создания всевозможных помех работе на компьютере. Признаки заражения: прекращение работы или неправильная работа ранее функционировавших программ медленная работа компьютера невозможность загрузки ОС исчезновение файлов и каталогов или искажение их содержимого изменение размеров файлов и их времени модификации уменьшение размера оперативной памяти непредусмотренные сообщения, изображения и звуковые сигналы частые сбои и зависания компьютера и др. Классификация компьютерных вирусов о среде обитания: Сетевые – распространяются по различным компьютерным сетям Файловые – внедряются в исполняемые модули (COM, EXE) Загрузочные – внедряются в загрузочные сектора диска или сектора, содержащие программу загрузки диска Фалово-загрузочные – внедряются и в загрузочные сектора и в исполняемые модули По способу заражения: Резидентные – при заражении оставляет в оперативной памяти компьютера свою резидентную часть, которая потом перехватывает обращения ОС к объектам заражения Нерезидентные – не заражают оперативную память и активны ограниченное время По воздействию: Неопасные – не мешают работе компьютера, но уменьшают объем свободной оперативной памяти и памяти на дисках Опасные – приводят к различным нарушениям в работе компьютера Очень опасные – могут приводить к потере программ, данных, стиранию информации в системных областях дисков По особенностям алгоритма: Паразиты – изменяют содержимое файлов и секторов, легко обнаруживаются Черви – вычисляют адреса сетевых компьютеров и отправляют по ним свои копии Стелсы – перехватывают обращение ОС к пораженным файлам и секторам и подставляют вместо них чистые области Мутанты – содержат алгоритм шифровки-дешифровки, ни одна из копий не похожа на другую Трояны – не способны к самораспространению, но маскируясь под полезную, разрушают загрузочный сектор и файловую систему Основные меры по защите от вирусов

	оснастите свой компьютер одной из современных антивирусных программ: Doctor Weber, Norton Antivirus, AVP постоянно обновляйте антивирусные базы делайте архивные копии ценной для Вас информации (гибкие диски, CD) Классификация антивирусного программного обеспечения Сканеры (детекторы). Принцип работы антивирусных сканеров основан на проверке файлов, секторов и системной памяти и поиске в них известных и новых (неизвестных сканеру) вирусов. Мониторы. Это целый класс антивирусов, которые постоянно находятся в оперативной памяти компьютера и отслеживают все подозрительные действия, выполняемые другими программами. С помощью монитора можно остановить распространение вируса на самой ранней стадии. Ревизоры. Программы-ревизоры первоначально запоминают в специальных файлах образы главной загрузочной записи, загрузочных секторов логических дисков, информацию о структуре каталогов, иногда - объем установленной оперативной памяти. Программы-ревизоры первоначально запоминают в специальных файлах образы главной загрузочной записи, загрузочных секторов логических дисков, информацию о структуре каталогов, иногда - объем установленной оперативной памяти. Для определения наличия вируса в системе программы-ревизоры проверяют созданные ими образы и производят сравнение с текущим состоянием.
Контрольный тест	Ответьте на вопросы и задания – Запишите признаки заражения ПК вирусом. – Проанализируйте и запишите, какие типы файлов подвержены заражению?

Дата___04.05.2021_____ _____ _____

Подпись Ф.И.О. преподавателя

Информация для размещения на официальном сайте ГБПОУ «Светлоградский региональный сельскохозяйственный колледж»

Для электронного обучения

Группа	321
Дата	07.05.2021г
Время	08-10-09-30
Наименование УД/МДК/УП/ПП	МДК 02.01
Ф.И.О. преподавателя	Сахарчук Т.В.
Электронная почта	saharchyk777@mail.ru
Основная литература	1. Федорова Г.Н. Разработка и администрирование баз данных (2-е изд., стер.) учебник«Академия»2020 г. 2. Федорова Г.Н. Информационные системы (6-е изд., стер.) учебник «Академия» 2018г 3. Рудаков А.В. Технология разработки программных продуктов (12-е изд.) учебник«Академия»2018 г. 4. Фёдорова Г.Н. Основы проектирования баз данных (2-е изд., стер.) учебник «Академия»2018г. 5. Основы проектирования приложений баз данных Баженова И.Ю. Интуит НОУ 2016 https://www.book.ru/book/917912 6. Базы данных. (СПО). Учебник Кумскова И.А. КноРус 2019 https://www.book.ru/book/932018
Тема № 119-120	Практическое занятие на тему: Защита информации
Задание	Цель занятия – Получение знаний о методах защиты информации, которым подвергаются компьютерные системы и потерях банков. Изучение основных понятий и определений, используемых при изучении дисциплины. 1.Теоретический материал Одним из наиболее эффективных методов обеспечения информационной безопасности являются организационно-технические методы. Что такое организационно-технические методы обеспечения информационной безопасности? Прежде всего, создание и совершенствование системы обеспечения информационной безопасности, разработка, использование и совершенствование СЗИ и методов контроля их эффективности. Этот этап тесно связан с правовыми методами защиты информации, такими как лицензирование (деятельности в области защиты информации), сертификация средств защиты информации и применение уже сертифицированных, и аттестация объектов информатизации по требованиям безопасности информации. А так же организационно технические методы связаны с экономическими, включающими в себя разработку программ обеспечения информационной безопасности Российской Федерации, определение порядка их финансирования, совершенствование системы финансирования работ, связанных с реализацией правовых и организационно-технических методов защиты информации, создание системы страхования

	информационных рисков. Защита информации всегда является комплексным мероприятием. В совокупности, организационные и технические мероприятия позволяют предотвратить утечку информации по техническим каналам, предотвратить несанкционированный доступ к защищаемым ресурсам, что в свою очередь обеспечивает целостность и доступность информации при ее обработке, передаче и хранении. Так же техническими мероприятиями могут быть выявлены специальные электронные устройства перехвата информации, установленные в технические средства и защищаемое помещение. Меры по охране конфиденциальности информации, составляющей коммерческую тайну (ФЗ 2004 г. № 98-ФЗ) определение перечня информации, составляющей коммерческую тайну; ограничение доступа к информации, составляющей коммерческую тайну, путем установления порядка обращения с этой информацией и контроля за соблюдением такого порядка; учёт лиц, получивших доступ к информации, составляющей коммерческую тайну, и (или) лиц, которым такая информация была предоставлена или передана; регулирование отношений по использованию информации, составляющей коммерческую тайну, работниками на основании трудовых договоров и контрагентами на основании гражданско-правовых договоров; нанесение на материальные носители (документы), содержащие информацию, составляющую коммерческую тайну, грифа "Коммерческая тайна" с указанием обладателя этой информации (для юридических лиц - полное наименование и место нахождения, для индивидуальных предпринимателей - фамилия, имя, отчество гражданина, являющегося индивидуальным предпринимателем, и место жительства). Если говорить об экономической стороне защиты информации, всегда важно одно правило – стоимость системы защиты информации не должна превышать стоимость этой информации. Но это не единственное «но» в этом вопросе. Нецелесообразно защищать всю информацию, какую можем, и все каналы информации какие только есть. Для этого необходимо определить объект защиты. Основными объектами защиты являются речевая информация и информация обрабатываемая техническими средствами. Так же информация может быть представлена в виде физических полей, информативных электрических сигналов, носителей на бумажной, магнитной, магнито-оптической и иной основе. В связи с этим защите подлежат средства и системы информатизации, участвующие в обработке защищаемой информации (ОТСС), технические средства и системы, не обрабатывающие непосредственно информацию, но размещенные в помещениях, где она обрабатывается (ВТСС) и защищаемые помещения. Практическое задание

	Ход выполнения работы: Скопировать папку Y:\ИБ на диск S:\ Создать в папке S:\ИБ каталоги 1, 2, 3, 4. Запустить программу ArtMasker.exe В диалоговом режиме выполнить все рекомендации Мастера (в качестве файла-контейнера выбрать) S:\ИБ\фото\Sky_01.bmp, в качестве маскируемого файла выбрать S:\Virus.doc, задайте параметры скрытия как средние Сохраните замаскированный файл с именем Security_1.bmp в папке S:\ИБ\1 Выполнить обратные действия ,сохранив размаскированный файл с именем Decod_1.doc в папке S:\ИБ\1 Переписать в тетрадь текст по описанию ArtMasker: ArtMasker - эта программа может прятать информацию в рисунки (BMP 8bit, 16bit, 32bit) и музыкальные файлы(WAV 8bit 16bit). Уникальная возможность этой программы - установка параметров скрытия. Файл-контейнер не меняет своего размера. Имеется поддержка мультиязычности. Запустить программу SimPass. Создать 5 паролей при помощи генератора, количество букв в пароле 10 (использовать специальные символы и латинские буквы). Выбрать любой понравившийся пароль и скопировать его в буфер. Запустить программу Secret BMP (в качестве пароля использовать пароль – результат работы генератора паролей) Создать небольшой!!!! растровый рисунок компьютерного вируса в редакторе PAINT, сохранив его с именем S:\ИБ\2\Pic.bmp Скрыть файл Pic.bmp в файле S:\ИБ\фото\Sky_02.bmp, сохранив новый файл с именем Security_2.bmp в папке S:\ИБ\2(использовать сгенерированный пароль) Выполнить обратные действия, сохранив извлеченный файл с именем Decod_2.bmp в папке S:\ИБ\2 Переписать в тетрадь текст по описанию Secret BMP и Simple Passwords: Secret BMP - реализация методов стеганографии и криптографии для защиты данных, хранящихся в файлах любого формата. Методы стеганографии применяются для скрытия секретных данных внутри файла-контейнера. В качестве файла контейнера используются файлы растровых изображений формата bmp. Перед скрытием файла в файле-контейнере (bmp-картинке) файл шифруется с использованием метода гаммирования. Для получения гаммы в работе используется 32-разрядный генератор случайных чисел, который программно реализуем и позволяет получать псевдослучайное число. Simple Passwords - программа для генерирования одновременно нескольких паролей из случайных символов. Позволяет выбрать символы, из которых должен состоять пароль - английские и русские, строчные и прописные, цифры и специальные. Можно указать количество символов в пароле и общее количество генерируемых паролей. Запустить программу CriptograFF для реализации криптозащиты из файла в файл Открыть файл для шифрования S:\ИБ\VIP.txt

	Зашифровать данный файл, присвоив ему имя S:\ИБ\3\Security_3.scr Выполнить обратные действия, сохранив расшифрованный файл с именем Decod_3.txt в папке S:\ИБ\3 Выполнить криптозащиту открытых файлов В окне программы набрать текст, где перечислить программно-технические средства защиты информации Зашифровать открытый файл с именем S:\ИБ\3\Metod.txt Переписать в тетрадь текст по описанию CriptograFF CriptograFF -шифрует текстовые файлы криптографическим методом. Предназначена для шифрования текстовых файлов по алгоритму RC4. Особенности данного алгоритма - большая скорость, возможность потокового шифрования, практическая невозможность вскрытия зашифрованного файла. Запустить программу Signature Cryptographer Зашифруйте файл S:\ИБ\фото\Sky_04.bmp, выбрав в качестве файла-ключа любой свой файл Сохраните этот файл с именем S:\ИБ\\4\Security_4 Выполнить обратные действия, сохранив извлеченный файл с именем Decod_4.bmp в папке S:\ИБ\\4 Переписать в тетрадь текст по описанию Signature Cryptographer: Signature Cryptographer - программа защиты информации в важных файлах от несанкционированного доступа. Шифровальщик использует в качестве ключа содержимое файлов вместо строки пароля. Таким образом, длина пароля может достигать гигантских размеров или вовсе быть больше длины шифруемого файла, что делает зашифрованный файл теоретически не взламываемым. Вместо длинных строк пароля запомнить нужно только имя файла, используемого для пароля.
Контрольный тест	Показать работу преподавателю, получить оценку

Дата___07.05.2021_____ _____ _____

Подпись Ф.И.О. преподавателя

Информация для размещения на официальном сайте ГБПОУ «Светлоградский региональный сельскохозяйственный колледж»

Для электронного обучения

Группа	321
Дата	07.05.2021г
Время	11-40-13-00
Наименование УД/МДК/УП/ПП	МДК 02.01
Ф.И.О. преподавателя	Сахарчук Т.В.
Электронная почта	saharchyk777@mail.ru
Основная литература	1. Федорова Г.Н. Разработка и администрирование баз данных (2-е изд., стер.) учебник«Академия»2020 г. 2. Федорова Г.Н. Информационные системы (6-е изд., стер.) учебник «Академия» 2018г 3. Рудаков А.В. Технология разработки программных продуктов (12-е изд.) учебник«Академия»2018 г. 4. Фёдорова Г.Н. Основы проектирования баз данных (2-е изд., стер.) учебник «Академия»2018г. 5. Основы проектирования приложений баз данных Баженова И.Ю. Интуит НОУ 2016 https://www.book.ru/book/917912 6. Базы данных. (СПО). Учебник Кумскова И.А. КноРус 2019 https://www.book.ru/book/932018
Тема № 121-122, 123-124	Лекция на тему: Сетевые, программные и технические средства информационных сетей
Задание	Системные программные средства, управляющие процессами в компьютерных сетях, объединенные общей архитектурой, определенными коммуникационными протоколами и механизмами взаимодействия вычислительных процессов, называются сетевыми операционными системами. Они предназначены для эффективного решения задач распределенной обработки данных, т.е. обработки данных не на отдельном локальном компьютере, а на нескольких объединенных сетью, причем часто бывает неважно - локальной или глобальной. Сетевые операционные системы ограничены областью своего действия. Сетевые супервизоры (управляющие программы) поддерживают работу одной или нескольких взаимодействующих локальных сетей. Если взаимодействуют несколько сетей (организована интерсеть), то сетевое программное обеспечение реализуется также в шлюзах и мостах, связывающих эти сети, а все сетевые объекты (рабочие станции, серверы), принадлежащие разным сетям, подчиняются общему адресному пространству. Сетевые операционные системы, поддерживая распределенное выполнение процессов, их взаимодействие, обмен данными между процессорами, доступ пользователей к общим ресурсам и другие функции, выполняют важные системные требования к распределенной системе как к целостной и многопользовательской. Требования к сетевым операционным системам. Различают следующие системные требования:

	единая системная архитектура. обеспечение требуемого высокого уровня прозрачности. высокоуровневая и высоконадежная файловая система. Единая системная архитектура.Понятие "системная архитектура" охватывает следующие вопросы: распределение функций между узлами сети; принципы построения коммуникационных протоколов; методы выполнения отдаленных операций типа «клиент-сервер»; структуру сетевой файловой системы; уровни прозрачности доступа к сети; принципы защиты данных; свойства общесетевого адресного пространства. Примером может служить адресация в Internet. Обеспечение требуемого высокого уровня прозрачности.Сетевая операционная система должна обеспечивать для пользователей доступ к многообразным сетевым ресурсам независимо от степени распределенности, неоднородности и мобильности данных, программ и устройств. Высокий уровень прозрачности означает, что обеспечиваются прозрачность доступа, прозрачность имен, прозрачность физических устройств и сетевой среды и т.д. Сетевая операционная система изолирует от пользователя все различия, особенности и физические параметры привязки процессов к обрабатываемым сетевым ресурсам. Например, пользователь может обратиться к процессу печати определенных данных, называя их уникальными составными именами, но совершенно не заботится о том, где практически находятся эти данные, и на каком физическом принтере они будут распечатаны. Высокоуровневая и высоконадежная файловая система.Файловая система, поддерживаемая сетевой операционной системой и входящая в ее состав, должна эффективно организовать хранение информации общего пользования и обеспечивать одновременный доступ к ней многих пользователей. Высокоуровневость означает, что доступ обеспечивается как к локальным файлам (расположенным на рабочих станциях), так и к удаленным (на серверах) на различных уровнях (справочник файлов; файл; именованный блок; сегмент файла). В сетевом режиме должны поддерживаться разнообразные операции с файлами (читать, писать, удалять, модифицировать). Протокол удаленного доступа и управления файлами должен обеспечивать все необходимые сетевые функции создания, обработки, пересылки и защиты файла. Файловая система - центральный элемент сетевой операционной системы, определяющий производительность и надежность всей распределенной системы в целом. Возможны следующие варианты структур сетевых операционных систем (СОС) ЛВС: каждая ЭВМ сети реализует все функции СОС, т.е. хранит в своей ОП резидентную часть СОС и имеет доступ к любой нерезидентной части, хранящейся на внешних носителях; каждая ЭВМ сети имеет копии программ только часто реализуемых функций СОС, копии программ редко реализуемых функций имеются в памяти только одной (или нескольких) ЭВМ;

	каждая ЭВМ сети выполняет только определенный набор функций СОС, причем этот набор является либо индивидуальным, либо неко-торые функции будут общими для нескольких ЭВМ. Различия в структурах СОС обусловлены принятыми способами управления ЛВС (децентрализованное или централизованное управ-ление). Отличительной особенностью СОС ЛВС является наличие слоя операционных систем, обеспечивающего обмен информацией между ЭВМ сети. Программное обеспечение локальных сетей. После подключения компьютеров к сети необходимо установить на них специальное сетевое программное обеспечение. Существует два подхода к организации сетевого программного обеспечения: сети с централизованным управлением; одно-ранговые сети. Сети с централизованным управлением. В сети с централизованным управлением выделяются одна или несколько машин, управляющих обменом данными по сети. Диски выделенных машин, которые называются файл-серверами, доступны всем остальным компьютерам сети. На файл-серверах должна работать специальная сетевая операционная система. Обычно это мультизадачная OS, использующая защищенный режим работы процессора. Остальные компьютеры называются рабочими станциями. Рабочие станции имеют доступ к дискам файл-сервера и совместно используемым принтерам, но и только. С одной рабочей станции нельзя работать с дисками других рабочих станций. С одной стороны, это хорошо, так как пользователи изолированы друг от друга и не могут случайно повредить чужие данные. С другой стороны, для обмена данными пользователи вынуждены использовать диски файл-сервера, создавая для него дополнительную нагрузку. Есть, однако, специальные программы, работающие в сети с централизованным управлением и позволяющие передавать данные непосредственно от одной рабочей станции к другой минуя файл-сервер. Пример такой программы - программа NetLink. После ее запуска на двух рабочих станциях можно передавать файлы с диска одной станции на диск другой, аналогично тому, как копируются файлы из одного каталога в другой при помощи программы Norton Commander. На рабочих станциях должно быть установлено специальное программное обеспечение, часто называемое сетевой оболочкой. Это обеспечение работает в среде той OS, которая используется на данной рабочей станции, - DOS, OS/2 и т.д. Файл-серверы могут быть выделенными или невыделенными. В первом случае файл-сервер не может использоваться как рабочая станция и выполняет только задачи управления сетью. Во втором случае параллельно с задачей управления сетью файл-сервер выполняет обычные пользовательские программы в среде MS-DOS. Однако при этом снижается производительность файл-сервера и надежность работы всей сети в целом, так как ошибка в пользовательской программе, запущенной на файл-сервере, может привести к остановке работы всей сети. Поэтому не рекомендуется использовать невыделенные файл-серверы, особенно в

	ответственных случаях. Существуют различные сетевые OS, ориентированные на сети с централизованным управлением. Самые известные из них - Novell NetWare, Microsoft Lan Manager (на базе OS/2), а также выполненная на базе UNIX System V сетевая OS VINES.
Контрольный тест	Ответьте на вопросы и задания 1. Что такое компьютерная сеть? 2. Что необходимо для создания компьютерных сетей? 3. Какова основная задача, решаемая при создании компьютерных сетей? 4. Что такое протоколы? Для чего они предназначены? 5. По какому принципу компьютерные сети делятся на локальные и глобальные? 6. Что такое интерфейсы? 7. Что такое серверы сети? 8. Какие сети называются одноранговыми? 9. Что такое рабочие станции? 10. Какие кабели можно использовать в качестве передающей среды в проводных сетях? 11. Что используются в качестве передающей среды в беспроводных локальных сетях? 12. Что представляет технология Ethernet? 13. Что такое сетевой адаптер? 14. Какие вы знаете топологии сетей? 15. Каковы преимущества беспроводных локальных сетей? 16. Каково назначение точки доступа? 17. Чем отличаются сети с выделенным сервером от одноранговых сетей? 18. Что такое технология клиент-сервер? 19. Приведите примеры сетевых операционных систем.

Дата___07.05.2021_____ _____ _____

Подпись Ф.И.О. преподавателя