ОРГАНИЗАЦИЯ ПРОЕКТНОЙ ДЕЯТЕЛЬНОСТИ ПРИ ИЗУЧЕНИИ ДИСЦИПЛИНЫ «ИНФОРМАЦИОННЫЕ ТЕХНОЛОГИИ В УПРАВЛЕНИИ КАЧЕСТВОМ И ЗАЩИТА ИНФОРМАЦИИ»

Габдуллина О.Г.
Оренбургский государственный университет, г. Оренбург

Федеральным государственным образовательным стандартом высшего профессионального образования по направлению подготовки 221400.62 Управление качеством предусмотрено изучение дисциплины «Информационные технологии в управлении качеством и защита информации». Данная дисциплина необходима для осознания студентами важности информации в управлении качеством и в управлении организацией в целом и необходимости использования технологий управления информацией.

Современное состояние мировой экономики характеризуется широким внедрением прикладных информационных технологий в области управления качеством. Несмотря на все возрастающие усилия по созданию технологий защиты данных, сохраняется тенденция к возрастанию их уязвимости, что делает необходимым ознакомление обучающихся с организационными, техническими, алгоритмическими и другими методами и средствами защиты компьютерной информации, с законодательством и стандартами в этой области.

Компьютерные информационные технологии позволяют автоматизировать процессы управления информацией и сократить время на выполнение всех функций организации. Поэтому в рамках данной дисциплины студенты знакомятся с основными информационными технологиями и программными продуктами, которые могут быть применены в менеджменте качества. Вторая составляющая дисциплины посвящена защите информации, которая является актуальной и обусловлена важностью и ценностью информации.

Широкое внедрение информационных технологий привело к появлению новых угроз безопасности людей. Это связано с тем обстоятельством, что информация, создаваемая, хранимая и обрабатываемая средствами вычислительной техники, стала определять действия большей части людей и технических систем. Как показывает практика, несанкционированный доступ представляет одну из наиболее серьёзных угроз для злоумышленного завладения защищаемой информацией в современных автоматизированных системах обработки данных. По нашему мнению, особое внимание необходимо уделить рассмотрению вопросов защиты информации в персональных компьютерах (ПК), так как

– основная часть персональных компьютеров расположена непосредственно на рабочих местах специалистов, что создает благоприятные условия для доступа к ним посторонних лиц;

– многие ПК служат коллективным средством обработки информации, что обезличивает ответственность, в том числе и за защиту информации;

– современные ПК оснащены накопителями большой емкости и способны сохранять информацию, будучи обесточенными;

– ПК ориентированы в большей степени на работу одного пользователя, поэтому изначально для них не предусматривалось специальных средств защиты данных.

В содержании дисциплины должны быть отражены следующие механизмы защиты ПК от несанкционированного доступа:

– физическая защита ПК и носителей информации;

– аутентификация пользователей и используемых компонентов обработки информации;

– разграничение доступа к элементам защищаемой информации;

– криптографическое закрытие защищаемой информации, хранимой на носителях;

– криптографическое закрытие защищаемой информации в процессе её непосредственной обработки;

– регистрация всех обращений к защищаемой информации. Количество часов регламентируется рабочей программой дисциплины.

Современные версии операционных систем (ОС) Windows в качестве основных инструментов обеспечения безопасности используют учетные записи; группы; права; разрешения и аудит безопасности. Учетная запись идентифицирует пользователя по системному имени и паролю, которые должны быть правильно набраны при входе в компьютер. Пользователи создаются либо ОС, либо административно. Для администрирования более удобна группа пользователей, так как пользователю, входящему в систему с учетной записью члена группы, обеспечивается автоматическое наследование прав, назначенных этой группе. Права пользователей, являющихся членами нескольких групп, суммируются. Встроенными группами локальной сети могут быть «Администраторы», «Опытные пользователи», «Пользователи», «Операторы архива», «Репликатор», «Гости», «Все» и специальные группы.

Права определяют круг полномочий, которые ОС делегируют пользователям и группам. Полный набор прав предоставлен системному администратору, которым может являться и владелец ПК. Остальным пользователям и группам предоставляются ограниченные права. Для встроенных групп и пользователей права устанавливаются автоматически, для остальных групп и пользователей права устанавливаются администратором. Права пользователей разделяются на привилегии и права входа в систему. Применяются права к учетным записям пользователей и групп. К компьютерным ресурсам применяются разрешения. Основные разрешения для работы с дисками и файлами: полный доступ, изменение, чтение и выполнение, чтение, запись. Для дисков и папок дополнительное разрешение – список содержимого папки; разрешение на удаление, удаление подпапок и файлов. Для работы с принтером существуют разрешения на печать, управление принтером и документами. Всего в файловой системе NTFS предусмотрено около 15 разрешений, устанавливаемых администратором и владельцами ресурсов.

Разрешения на ресурс, выданные группе, могут наследоваться всеми пользователями данной группы. В то же время, владелец ресурса может запретить разрешения на наследование (флажки *Разрешить* и *Запретить* в окне *Безопасность ресурса*). В таких случаях возможны конфликты между правами и разрешениями, разрешениями и запретами. В этом случае приоритет отдается праву, разрешению или запрету согласно системному протоколу приоритетов.

Для определения злоумышленников, пытающихся поставить под угрозу системные и пользовательские данные, в ОС предусмотрены аудиты безопасности:

- вход в систему;
- управление учётными записями;
- доступ к службе каталогов;
- доступ к объектам;
- изменение политики безопасности;
- использование привилегий;
- отслеживание процессов;
- системные события.

Аудиты включаются или выключаются в параметрах безопасности Windows (Локальные политики/Политика аудита). В каждом включенном аудите можно задать проверку успехов или отказов: аудит успехов означает создание записи аудита при каждой успешной попытке, аудит отказов – при каждой неудачной. Включенный аудит фиксирует соответствующие события в журналах безопасности, приложений и системном журнале. Эти журналы доступны в окне просмотра событий. В современных версиях ОС используются утилиты безопасности, обеспечивающие криптографическую защиту файлов; восстановление повреждённых данных и системных файлов; защиту от вирусов и нежелательной Internet - информации; защиту системных файлов от несанкционированных попыток их замены или перемещения.

Приложения MS Office (совместно с Windows) обладают рядом простейших и эффективных защитных средств, доступных любому пользователю. Стратегия безопасности данных в MS Office двухуровневая. На пользовательском уровне офисные приложения совместно с Windows предоставляют пользователю меры защиты папок и файлов в рамках прав пользователя и разрешений на ресурсы. На этапе сохранения файлов возможна организация системной защиты папок, содержащих эти файлы. Эта технология реализуется непосредственно в окнах сохранения файлов, если пользователь наделён соответствующими правами. Вне своих прав пользователь может обратиться к системному уровню под контролем и с разрешения администратора сети или компьютера. Такая стратегия является оптимальной для решения практических задач безопасности в многопользовательском режиме работы.

Для практической реализации и приобретения навыков защиты данных от несанкционированного доступа и чтения обучающимся может быть

предложена работа над проектом. Организация проектной деятельности является одной из перспективных инновационных образовательных технологий, интегрирующей в себе проблемный подход, групповые методы, рефлексивные, презентативные, исследовательские, поисковые подходы. Учебный проект дает обучающемуся возможность решить интересную проблему, максимально используя свои возможности, попробовать свои силы, приложить знания и показать публично достигнутый результат. Учебный проект позволяет вырабатывать и развивать следующие компетентности:

- постановка задач;
- целеполагания и планирования деятельности;
- применение знаний, умений и навыков в различных ситуациях;
- презентации деятельности и её результатов.

Рассмотрим технологию предлагаемого учебного проекта.

Тема: Защита данных от несанкционированного доступа и чтения.

Цель: Изучение средств и методов защиты информации в персональных компьютерах от несанкционированного доступа и чтения.

Задачи:

1.Освоить средства системной защиты данных: скрытие файлов и папок, сетевая и локальная политики доступа (уровни пользователя и менеджера группы), защита приложений (Word, Excel, Access) от сетевого и локального доступа, блокировка компьютера.

2. Освоить средства парольной защиты офисных приложений

3. Освоить стандартные средства скрытия фрагментов данных в офисных приложениях.

4. Освоить технологию криптографической защиты файлов.

5. Провести сравнительную оценку эффективности архиваторов, используемых в файловых мониторах Windows.

6. Подготовить отчёт о проделанной работе в PowerPoint.

Необходимые материалы, оборудование и программное обеспечение: задание, папки, документы Word, таблицы Excel, базы данных Access, OS Windows, Microsoft Office, персональный компьютер.

Продолжительность: 2 недели.

Ход работы над проектом:

Исследовательская проблема, лежащая в основе проекта - роль и место общесистемных технологий защиты информации в системе менеджмента качества. На практических занятиях по изучению дисциплины студентами создаются документы, таблицы, базы данных, содержащих информацию о качестве, которые далее используются в проекте для отработки навыков системной, парольной, криптографической защиты данных. Особенностью информации, обрабатываемой в рамках системы менеджмента качества, является её разнородность. Некоторые типы информации существую в виде документов (нормативные документы, правила и процедуры, должностные инструкции); другие типы информации существуют в виде данных о продукции, потребителях, материалах, что обуславливает использование различных программных систем для её обработки. С повышением значимости

и ценности информации растёт и важность её защиты. В ряде случаев достаточно, чтобы пользователь был уверен в достаточной надёжности защиты.

С помощью *локальной политики безопасности*, управляемой системным администратором, можно защитить установки скрытия от взлома, которые делаются в два приема:

а) устанавливается атрибут *Скрытый* для выделенного файла (группы файлов) или папки;

б) устанавливается запрет на показ файлов и папок с атрибутом *Скрытый*.

После выполнения указанных операций скрытые файлы и папки не видны для постороннего глаза в файловых списках, в том числе в окнах поиска файлов. Чтобы получить доступ к скрытым файлам и папкам, достаточно снять запрет на их показ:

а) включить переключатель *Показывать скрытые файлы и папки;*

б) включить флажок *Показывать скрытые/системные файлы (только для опытных).*

Права опытного пользователя позволяют ему управлять доступом и к обозреваемым ресурсам, прежде всего к своим папкам, в которых содержатся файлы с данными.

Не следует открывать без необходимости общий сетевой доступ к папке с ответственными данными, иначе с любой рабочей станции сети эта папка будет видна всем пользователям, допущенным к работе на этой станции. Если служебная необходимость заставляет сделать папку общедоступной, можно ограничить число допущенных пользователей и разрешений на доступ к данным как показано на рисунке 1.

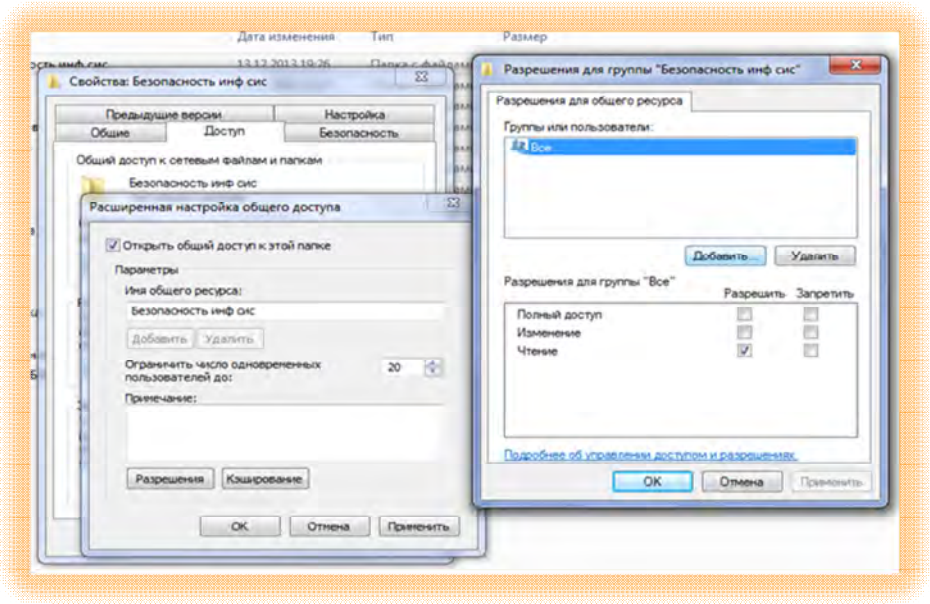

Рисунок 1 – Установки окна доступа к ресурсам.

В окне доступа следует переключатель поставить в положение *Открыть общий доступ к этой папке* и ввести предельное число допущенных пользователей.

Следующий этап – выдача разрешений (нажать кнопку *Разрешения* - *рисунок 2*). В появившемся окне следует удалить группу *Все* (кнопка *Удалить*) и с помощью кнопки *Добавить* перейти к организации своей группы.

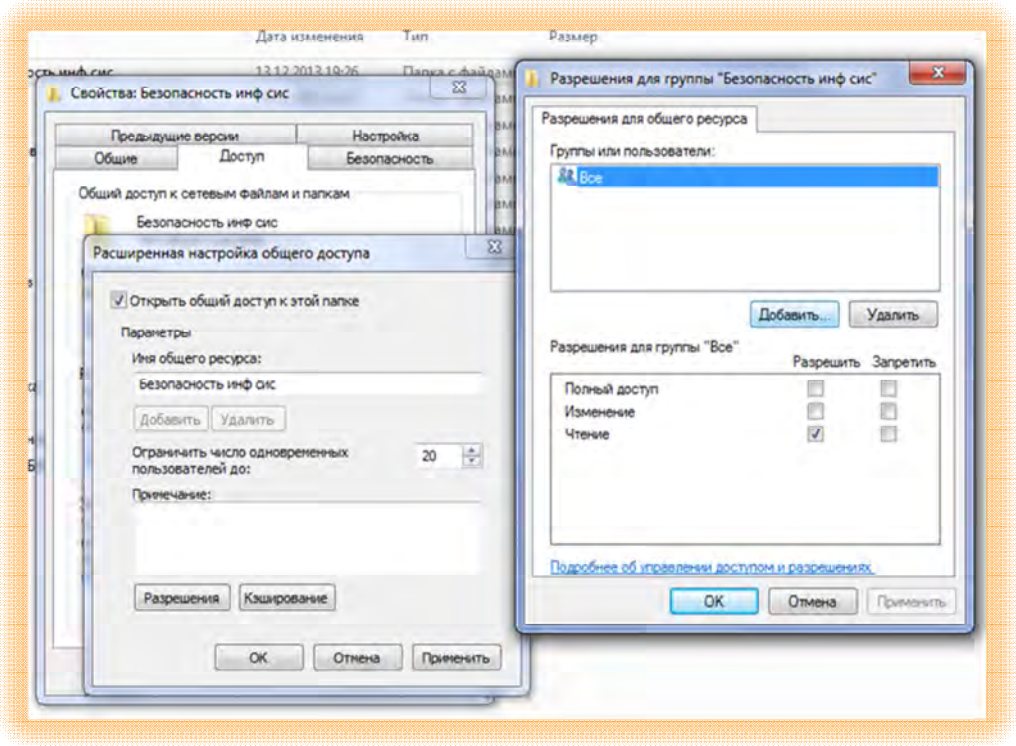

Рисунок 2 – Окно выдачи разрешений.

В окне разрешений каждому члену группы оформляем тип доступа к папке. Если все они будут равноправно вводить данные в файлы этой папки, надо, либо разрешить полный доступ к папке, либо разрешить редактирование. Из окна разрешений выходим в окно свойств и закрепляем все сделанные выше установки коллективного доступа. Теперь папка, в которой будет создаваться коллективная база данных, доступна всем членам группы в пределах индивидуальных разрешений, установленных менеджером группы. Посторонние лица (кроме системного администратора) к данной папке не имеют доступа с других рабочих станций.

Если компьютер используется локально несколькими пользователями, то необходимо создать учетные записи пользователей. Затем включить режим безопасности, для чего следует войти в опцию *Пуск/Панель управления/Свойства папки* и в окне вкладки *Вид* снять флажок *Использовать простой общий доступ к файлам (рекомендуется*). В результате в свойствах папок и файлов появится вкладка *Безопасность*. Войдя по этой вкладке в окно безопасности, мы увидим окно с увеличенным числом разрешений – рисунок 3.

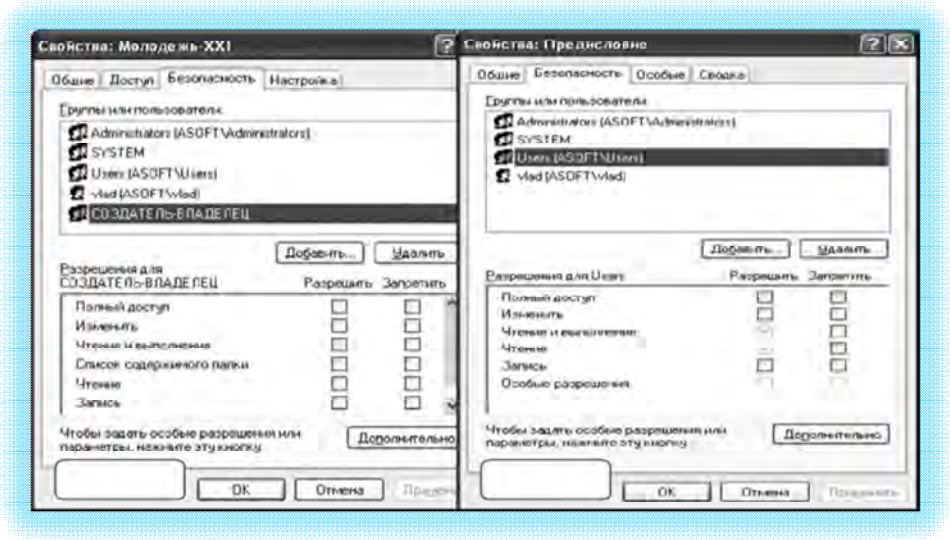

Рисунок 3 - Окно разрешений.

В Word и Excel в *Окне сохранения файла* через *Файл/Общий доступ/Доступ* или *Параметры сохранений/Общие параметры* выходим на уже рассмотренные окна системного доступа и безопасности.

Поскольку в Access местоположение сохраняемого файла новой базы данных определяется на самом первом этапе ее создания, описанная технология реализуется в окне создания файла БД.

Также в СУБД Access реализованы специфические меры защиты от несанкционированного доступа к конкретным объектам БД с дифференциацией по правам пользователей и разрешениям на объекты. Защитные операции для существующей базы данных Access производятся из меню Файл. Команда Мастер запускает мастер защиты БД –рисунок 4.

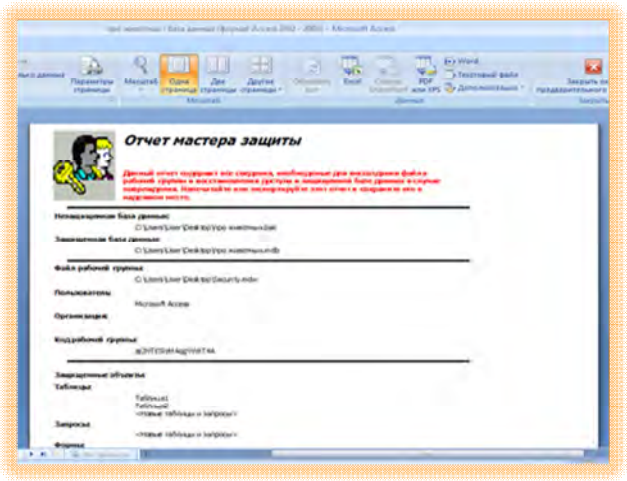

Рисунок 4 –Отчёт мастера защиты Access.

За 8 шагов мастер защиты, предварительно создав резервную копию БД, защищает базу данных дифференцированно по каждому из допущенных пользователей и групп пользователей и по объектам БД. Особо важные базы данных с высоким уровнем защиты рекомендуется создавать именно в Access.

Итоговый продукт: Презентация проекта.

После завершения работы над проектом проводится его защита в форме доклада с презентацией, подготовленной в PowerPoint.

Система оценки проектных работ представлена в таблице 1:

Таблица 1 Оценка проектных работ

№	Оцениваемый показатель	Количество баллов
1	Соответствие реализации задуманному проекту	1
2	Качество выполнения продукта	1
3	Умение раскрыть сущность реализованного проекта и его основные результаты	1
4	Умение отвечать на вопросы: лаконичность и аргументированность	1
5	Активность каждого автора проекта	1
Общая сумма баллов		

С системой оценок проектных работ студенты должны быть ознакомлены заранее. Проект может выполняться в группе либо самостоятельно.

С использованием метода проектов преподаватель не преподносит учебную информацию в готовом виде, а ставит перед обучающимися творческие проблемные задания, в процессе решения которых они должны приобрести новые знания. Учебная деятельность приобретает творческий, инновационный характер. Технология учебного проектирования направлена на развитие профессионально важных качеств и способностей будущих специалистов, на приобретение ими опыта квалифицированного выполнения профессиональной деятельности.

Список литературы

1. ***Гухман В.Б., Тюрина Е.И.*** *Основы защиты данных в Microsoft Office: Уч. пособие. 1-е изд. Тверь: ТГТУ, 2005. 100 с.*