УДК 378.147:004.056.52

МЕТОДИКА ПРЕПОДАВАНИЯ ТЕМЫ «ОРГАНИЗАЦИЯ ПАРОЛЬНОЙ ЗАЩИТЫ В ФАЙЛОВЫХ СИСТЕМАХ» ДЛЯ ОБУЧАЮЩИХСЯ НЕТЕХНИЧЕСКИХ СПЕЦИАЛЬНОСТЕЙ

Бакулин В.М., Еськин Д.Л.

ФГКОУ ВО «Волгоградская академия МВД России», Волгоград,
e-mail: bvm@volgodom.ru, yd38@bk.ru

В работе предложена разработанная авторами методика проведения практического занятия по теме «Организация парольной защиты в файловых системах». Данная методика направлена на формирование у обучающихся нетехнических специальностей элементов компетенции, связанной с обеспечением информационной безопасности в профессиональной деятельности, в части развития умений для предотвращения несанкционированного доступа к информации или ее злоумышленной модификации, путем установки парольной защиты на файлы пользователя. Методика позволяет развить умения установки ограничений на доступ к информации как с использованием средств операционных систем семейства Microsoft Windows, так и с использованием встроенных функций шифрования документов, имеющихся в современных пакетах офисных программ. Особое внимание в рассматриваемой работе уделяется методике формирования у обучающихся твердого убеждения в необходимости соблюдения элементарных требований безопасности при составлении паролей.

Ключевые слова: методика обучения, доступ к файлам, защита паролем, аутентификация

THE TECHNIQUE OF TRAINING OF THE THEME «ORGANIZATION OF PASSWORD PROTECTION IN FILE SYSTEMS» FOR STUDENTS OF NON-TECHNICAL SPECIALTIES

Bakulin V.M., Yeskin D.L.

Volgograd Academy of the Ministry of the Interior of the Russian Federation, Volgograd,
e-mail: bvm@volgodom.ru, yd38@bk.ru

The paper proposes a method of the practice session on the theme «Organization of password protection in the file systems» developed by the authors. This technique is aimed at competence elements developing of non-technical specialties students' related to information security in their professional activities, in terms of skills development in order to prevent unauthorized access to information or malicious modification, by setting password protection on the user's files. The technique allows to develop the ability to set restrictions on access to information as a means of using the Microsoft Windows operating systems and using the built-in document encryption functions available in modern office applications. Special attention is under consideration in the procedure given in the formation of students a firm conviction of the need to comply with basic safety requirements when selecting a password.

Keywords: training technique, access to files, protection by the password, authentication

В современном мире информация стала одним из наиболее ценных ресурсов человечества. Бурное развитие информационных технологий привело к тому, что колоссальный ее объем в настоящее время хранится в электронной форме и обрабатывается средствами вычислительной техники. Это привело к возникновению новых путей несанкционированного доступа к информации, которыми могут воспользоваться злоумышленники. За 2015 год, по данным аналитического центра InfoWatch было официально зарегистрировано 1505 случаев утечки конфиденциальной информации [2]. 31,5% из них связаны с хищением информации по локальной сети либо сети Интернет, 15,9% – с хищением информации непосредственно со средств вычислительной техники, 3,6% – со съемных носителей информации. В связи с этим задача формирования у будущих специалистов элементов компетенции, связанной со способностью обеспечения защиты информации в профессиональной деятельности, в части развития умений для предотвращения несанкционированного доступа к информации или ее злоумышленной модификации, является весьма важной [1].

Одним из простейших методов, позволяющих ограничить доступ к документам, хранящимся в электронной форме, является организация парольной защиты файлов. Данный метод не может гарантировать стопроцентную защиту документа от угрозы ознакомления или модификации его злоумышленником, однако при соблюдении ряда требований к создаваемым паролям позволяет до нескольких десятков лет увеличить время, необходимое злоумышленнику для преодоления парольной защиты и, кроме того, не требует глубоких технических знаний от применяющего его специалиста. Последнее является немаловажным при обучении студентов нетехнических спе-

циальностей, федеральные государственные образовательные стандарты которых не предполагают глубокого изучения учебных дисциплин, в той или иной мере связанных с защитой информации.

При составлении методики проведения занятия, прежде всего, необходимо определиться с его формой. В качестве традиционных форм проведения занятий можно выделить следующие: лекция, семинарскоезанятие,практическое(лабораторное) занятие.

Каждая из указанных форм имеет свои преимущества и недостатки.

Классическое лекционное занятие представляет собой последовательное, структурированное, монологическое устное изложение лектором учебного материала, как правило, теоретического характера [6]. При этом достигается максимальная плотность изложения информации при минимальных временных затратах. К недостаткам данного вида занятия можно отнести почти полное отсутствие обратной связи, усредненный уровень сложности изучаемого материала, и, как следствие, разную степень вовлеченности обучающихся в учебный процесс.

Семинарское занятие предусматривает самостоятельную предварительную работу и обсуждение обучающимися вопросов, призванных обеспечить углубление, расширение и систематизацию знаний, выработку познавательных умений и формирование опыта творческой деятельности, и предназначено для подготовки обучающихся к самообразованию и творческому труду [5]. Преподаватель в данном случае выступает в роли координатора, направляя ход занятия в нужное русло. Благодаря постоянной обратной связи и высокой вовлеченности аудитории, можно достаточно точно контролировать процесс усвоения материала. Однако, стоит учитывать, что семинарские занятия проводятся в относительно небольших группах и от обучающихся требуется обязательная предварительная подготовка.

Практическое занятие – это вид учебного занятия, на котором педагогический работник организует прикладную деятельность по использованию освоенных теоретических положений учебной дисциплины и формирует опыт индивидуального решения обучающимися сформулированных задач [4].

Выбор формы занятия должен базироваться на тех целях, которые ставит перед собой преподаватель. Для рассматриваемой темы «Организация парольной защиты в файловых системах» с учетом нетехнической профессионально-профильной ориентации обучающихся можно выделить две основные цели:

1. Обзорно-ознакомительная – дать общие понятия и принципы организации парольной защиты доступа к данным.

2. Практико-ориентированная – освоить конкретные инструменты и программные продукты, которые позволяют пользователю без особой специальной подготовки научиться защищать свои данные посредством использования паролей.

С учетом обозначенных целей целесообразным является рассмотрение данной темы в рамках двух занятий: лекционного – в котором даются общие теоретические положения в области защиты информации, и практического – для непосредственного освоения методов организации парольной защиты.

Не будем останавливаться на методике чтения лекции, так как в данном случае будет достаточно классического подхода, а более подробно рассмотрим порядок проведения практического занятия.

Для начала необходимо определиться с основными требованиями, которые будут предъявляться к разрабатываемому практическому занятию:

- занятие должно иметь четкую структуру и, по возможности, должно быть разбито на отдельные логически завершенные этапы;
- каждое последующее задание должно являться логическим продолжением предыдущего;
- сложность выполняемых заданий в пределах одного этапа должна меняться по принципу «от простого к сложному»;
- при выполнении заданий от обучающихся не должно требоваться наличие специальных знаний в области защиты информации;
- чтобы не выйти за временные рамки, занятие не должно быть сильно перегруженным упражнениями;
- по возможности необходимо использовать в качестве инструментов обучения только свободно распространяемое или бесплатное программное обеспечение.

Для выполнения указанных требований структуру занятия предлагается разбить на три логически связанных этапа. Первый этап посвящен изучению особенностей защиты файлов через систему управления доступом операционных систем семейства Microsoft Windows. Второй этап связан с развитием у обучающихся умений установки парольной защиты файлов в офисных приложениях. Во время третьего этапа обучающиеся с помощью специализированных утилит производят подбор паролей к файлам офисных приложений. Рассмотрим содержание каждого из этапов более подробно.

Цель первого этапа занятия – освоение обучающимися навыков организации защиты информации, хранимой на рабочем компьютере, штатными средствами операционной системы.

Так как выполнение первого этапа связано с изменениями настроек операционной системы от имени администратора, то для начала необходимо обеспечить ее работоспособность даже в случае возможных ошибочных действий пользователей. Для этого наиболее простым и эффективным способом является использование виртуальной машины, такой как VirtualBox или подобной, которая позволяет полностью изолировать учебную систему от рабочей.

Таким образом, первое, с чего начнется выполнение задания для обучающегося, будет запуск программы виртуальной машины с записанным образом учебной операционной системы. Далее, войдя в систему от имени администратора и используя возможности системы управления учетными записями, обучающийся создает два различных профиля пользователей и для каждого пользователя устанавливает индивидуальный пароль.

После создания профилей обучающемуся предлагается осуществить вход в систему поочередно от имени каждого из пользователей и попытаться получить доступ к папке «Мои документы» другого пользователя, а затем проделать то же самое от имени администратора. В результате выполнения данного упражнения обучающийся должен будет понять, что задание паролей пользователей недостаточно для защиты информации от пользователей с правами администратора.

Для усиления парольной защиты предлагается воспользоваться встроенной в операционную систему функцией шифрования. Предполагается, что к этому занятию обучающиеся уже успели ознакомиться с основными принципами криптографического преобразования информации [3], и, в частности, с таким понятием, как ключ шифрования, который формируется операционной системой на основе пароля учетной записи пользователя.

Освоение механизма включения шифрования данных проводится последовательно сначала для отдельных файлов, а затем для папок. Обучающемуся предлагается войти в систему под учетной записью одного из пользователей, в любом месте диска создать произвольный файл и в свойствах файла установить параметр шифрования. После этого необходимо попытаться получить доступ к зашифрованному файлу от имени другого пользователя и от имени администратора. После выполнения данного упражнения обучающемуся предлагается сделать вывод о степени защиты файла в случае шифрования, и проделать такие же действия с папками, содержащими файлы.

Цель второго этапа занятия – развить у обучающихся умения установки парольной защиты на документы с помощью встроенных функций шифрования, имеющихся в пакетах современных офисных приложений. Данный этап занятия предполагает использование локальной сети и текстового процессора, например, Microsoft Word или Open Office Writer. Для достижения поставленной цели используется следующая методика. Сначала обучающемуся предлагается, используя информационные ресурсы сети Интернет, а также справочную систему текстового процессора, найти информацию о том, каким образом в используемом в рамках занятия текстовом процессоре осуществляется установка пароля на открытие документа, а также устанавливаются ограничения на редактирование документа, в частности ограничение «только чтение» и разрешение на возможность записи исправлений. После этого обучающийся создает три документа, в которых в краткой форме указывает найденную им информацию и устанавливает на них соответствующую защиту, используя в качестве пароля сетевое имя своего компьютера. Эти три файла обучающийся копирует в папку на жестком диске, к которой предоставлен сетевой доступ. После этого обучающимся предлагается осуществить взаимную проверку друг друга, осуществляя доступ к файлам по сети, в ходе которой проверяется как правильность установки ограничений на доступ к содержимому файлов, так и правильность информации, содержащейся в них.

Цель третьего этапа занятия – сформировать у обучающихся твердое убеждение в необходимости соблюдения элементарных требований безопасности при составлении паролей. К этим требованиям относится, прежде всего, следующее:

- длина пароля должна составлять 6 и более символов;
- при составлении пароля следует использовать символы различных групп (прописные и строчные буквы, буквы различных языков, спецсимволы);
- при составлении пароля нельзя использовать производные от слов любого языка.

Данный этап занятия предполагает использование специализированных утилит для восстановления паролей к документам

офисных приложений, например, бесплатной утилиты FREE Word and Excel password recovery Wizard.

Для достижения поставленной цели предлагается использовать следующую методику. Обучающийся создает документ Microsoft Word произвольного содержания, после чего зашифровывает его паролем. Далее, используя утилиту подбора паролей, методом BruteForce осуществляет подбор пароля, измеряя при этом время, затраченное на данную процедуру. После чего обучающийся изменяет пароль и повторяет свои предыдущие действия. Сначала в качестве паролей предлагается последовательно использовать комбинации, состоящие из пяти, шести, семи и восьми цифр. Анализ полученных данных позволяет обучающемуся сделать вывод о влиянии длины пароля на скорость его подбора. Далее в качестве пароля используются комбинации из четырех, пяти и шести латинских строчных букв. В результате, сравнивая полученные в этом случае данные с предыдущими, обучающийся может сделать вывод о влиянии числа возможных для использования символов в пароле на его стойкость. В качестве последнего пароля предлагается использовать слово из шести букв на английском языке, а подбор его осуществлять двумя методами: сначала BruteForce, а затем используя «атаку по словарю». В итоге обучающийся может сделать вывод о недопустимости применения производных от слов любого языка в качестве пароля. Следует отметить необходимость варьирования числа символов, из которых составляются пароли, в зависимости от вычислительной мощности используемых на занятии ЭВМ.

После проведения всех измерений обучающемуся необходимо построить график, на котором изобразить две кривые, соответствующие цифровому и буквенному паролям. По оси абсцисс на графике откладывается число символов, из которых состоит соответствующий пароль, а по оси ординат – затрачиваемое на его подбор время. Далее в процессе группового обсуждения полученных данных обучающимся предлагается сформулировать единые базовые требования безопасности при составлении паролей.

После этого обучающимся предлагается составить для себя пароль с одной стороны легкий для запоминания, а с другой – отвечающий сформулированным требованиям безопасности. В заключение, используя специализированный сервис оценки стойкости пароля, например, портала 2ip.ru, обучающиеся оценивают его стойкость и при необходимости производят его коррекцию.

Предложенная методика проведения практического занятия по освоению методов организации парольной защиты не требует от обучающихся наличия глубоких специальных знаний в области обеспечения информационной безопасности в компьютерных системах, и в то же время она позволяет овладеть практическими навыками защиты информации, которые могут быть полезны для специалистов, работающих с конфиденциальными сведениями. Дополнительным плюсом предлагаемой методики является то, что все необходимое для проведения занятия программное обеспечение распространяется на бесплатной основе, либо имеет бесплатные аналоги.

Список литературы

1. Бакулин В.М. Основные вопросы информационной безопасности // Вестник Волгоградской академии МВД России. – 2010. – № 4. – С. 126–129.

2. Глобальное исследование утечек конфиденциальной информации в 2015 году [Электронный ресурс]. Режим доступа: URL: https://www.infowatch.ru/report2015 (дата обращения: 13.05.2016).

3. Еськин Д.Л., Бакулин В.М Оптимизация обучения по теме «Основы криптографии» обучающихся юридических специальностей. // Современные проблемы науки и образования. – 2015. – № 6; URL: http://www.science-education.ru/article/view?id=23102 (дата обращения: 13.05.2016).

4. Кононец Н.В. Практическое занятие по информатике в контексте ресурсно ориентированного обучения студентов // Фундаментальные исследования. – 2013. – № 11–3. – С. 540–545.

5. Профессиональная педагогика: Учебник для студентов, обучающихся по педагогическим специальностям и направлениям / Под ред. С.Я. Батышева, А.М. Новикова. Издание 3-е, переработанное. – М.: Из-во ЭГВЕС, 2009. – 456 с.

6. Чижик В.П. Инновационные способы активизации познавательной деятельности студентов при проведении лекционных занятий // Сибирский торгово-экономический журнал. – 2011. – № 14. – С. 110–119.