УДК 378.147:004.056.52

МЕТОДИКА ПРЕПОДАВАНИЯ ТЕМЫ «ЗАЩИТА ИНФОРМАЦИИ ШТАТНЫМИ СРЕДСТВАМИ ОПЕРАЦИОННОЙ СИСТЕМЫ» ДЛЯ ОБУЧАЮЩИХСЯ НЕТЕХНИЧЕСКИХ СПЕЦИАЛЬНОСТЕЙ

Бакулин В.М.[1], Еськин Д.Л.[1]

[1]ФГКОУ ВО «Волгоградская академия МВД России», Волгоград, e-mail: bvm@volgodom.ru

Работа имеет междисциплинарный характер, написана на стыке педагогики и информационной безопасности. Авторами предложена методика проведения практического занятия по теме «Защита информации штатными средствами операционной системы» для обучающихся, не обладающих глубокими техническими знаниями в области информационной безопасности. Рассматриваемая методика предполагает четыре этапа освоения учебного материала и способствует развитию умений организации парольной защиты информации, использования возможностей механизмов разграничения доступа к информации, применения штатных методов шифрования для усиления защиты, а также использования штатных механизмов восстановления системы. Особенностью предлагаемой методики является то, что все используемое программное обеспечение входит в состав операционных систем. Применение данной методики способствует эффективному формированию компонентов компетенций, связанных с защитой информации в профессиональной деятельности.

Ключевые слова: методика обучения, защита информации, парольная защита, разграничение доступа, шифрование, восстановление системы.

METHODS OF TEACHING THE TOPIC "SECURITY OF INFORMATION BY STANDARD MEANS OF OPERATING SYSTEM" FOR STUDENTS OF NON-TECHNICAL SPECIALTIES

Bakulin V.M.[1], Yeskin D.L.[1]

[1]Federal State Public Educational Institution of Higher Education "Volgograd Academy of the Internal Affairs Ministry of the Russian Federation", Volgograd, e-mail: bvm@volgodom.ru

The work has interdisciplinary character and is written at the crossroads of pedagogical and information security sciences. A methodology for holding the practical class on the theme "Security of information by means of standard operating system" for students that do not possess deep technical knowledge in the field of information security, is proposed. The teaching methodology involves four stages while training the educational material and promotes the development of skills of organization of password security of information and using the mechanisms of differentiation of access to information, and also using the standard encryption techniques to increase protection, and also the use of standard recovery mechanisms of the system. A peculiarity of methodology proposed is that all used software is a part of operating system. The application of this methodology contributes to the effective formation of the components of competences related to the security of information in their professional activities.

Keywords: training technique, information security, password protection, access isolation, enciphering, system recovery.

Сегодня информация является одним из ценнейших ресурсов человечества как в масштабах государства, так и отдельной личности. Глобальная информатизация всех сфер деятельности человека привела к существенному росту производительности труда. С другой стороны, возник целый ряд связанных с этим проблем. Одна из этих проблем - необходимость обеспечения информационной безопасности. В настоящее время колоссальный объем данных представляет собой информацию ограниченного доступа. К ней относятся различные виды тайн, таких как государственная тайна, коммерческая, банковская, врачебная, служебная и т.д. Практически любая организация занимается

обработкой персональных данных граждан, которые также подлежат защите [1]. В связи с этим достаточно остро стоит задача формирования у будущих специалистов компетенций, связанных со способностью обеспечения защиты информации в профессиональной деятельности.

Одним из базовых путей защиты информации является использование штатных функций операционных систем. Современные операционные системы обладают мощными встроенными средствами обеспечения безопасности, осуществляющими аутентификацию, авторизацию, аудит действий пользователей в системе, защиту от сбоев, криптографическую защиту объектов операционной системы, предотвращение сетевых атак [2]. Использование штатных функций операционной системы является доступным и не требует глубоких технических знаний от применяющего их специалиста. При обучении студентов нетехнических специальностей этот фактор является одним из ключевых, поскольку федеральные государственные образовательные стандарты данной категории обучающихся не предполагают глубокого изучения специализированных учебных дисциплин, направленных на формирование умений и навыков защиты информации.

Выбор методики подачи материала по заданной теме требует определиться с целями, количеством и формой проводимых занятий. Так, основной целью освоения темы «Защита информации штатными средствами операционной системы» является получение общих сведений о формах и методах защиты информации штатными средствами операционных систем, а также приобретение практических навыков по организации парольной и криптографической защиты информации, разграничению прав доступа для различных пользователей и штатному восстановлению работоспособности системы после сбоя.

С учетом обозначенных целей целесообразным является рассмотрение данной темы в рамках двух занятий: лекционного и практического. Лекционное занятие предлагается посвятить описанию общих принципов функционирования операционных систем и краткому обзору их штатных функций в области защиты информации. Практическое занятие предлагается полностью посвятить освоению основных наиболее простых и эффективных инструментов защиты информации, включенных в комплект поставки операционной системы.

Для методики проведения лекционного занятия по данной теме достаточно будет классического подхода с последовательным структурированным изложением материала и демонстрацией конкретных примеров. Поэтому более подробно остановимся на описании методики и порядка проведения практического занятия.

Главной особенностью описываемой методики проведения занятия является то, что обучающиеся должны иметь полный, не ограниченный доступ ко всем ресурсам

операционной системы, что, в свою очередь, означает необходимость предоставления обучающимся прав администратора системы. В связи с этим представляется необходимым изолирование учебной системы от основной системы рабочей станции, на которой планируется выполнение учебных заданий. Наиболее простым методом реализации полностью изолированной учебной системы является применение «виртуальных машин». Технология виртуальных машин позволяет убрать все ограничения и максимально приблизить имитационные эксперименты к реальным условиям эксплуатации систем [3]. При этом можно не опасаться за возможные неверные действия обучающихся, которые могли бы привести к нарушению работоспособности основной системы учебной рабочей станции. Таким образом, первое, с чего начинается описываемое практическое занятие, это запуск «Виртуальной машины» с установленной учебной операционной системой.

Перед тем как обучающиеся приступят к выполнению практических заданий, следует сформировать у них убежденность, что все приобретенные в ходе занятия умения и навыки пригодятся им в их дальнейшей профессиональной деятельности и в быту.

Структурно основную часть занятия можно разбить на четыре этапа:

1. Изучение возможностей организации парольной защиты данных пользователя.
2. Использование механизмов разграничения доступа к информации, локально хранящейся на компьютере.
3. Применение штатных методов шифрования для усиления защиты.
4. Изучение штатных механизмов восстановления системы.

На первом этапе занятия обучающиеся должны освоить основные приемы организации парольной защиты компьютера штатными средствами операционной системы. Для этого им предлагается выполнить следующий набор заданий:

1. Создать в системе двух дополнительных пользователей, присвоив им индивидуальные логины и пароли.
2. Войти в систему от имени одного из созданных пользователей и сохранить нескольких файлов в индивидуальных папках пользователя (например, в папке «Мои документы»), а также в произвольном месте на диске.
3. Войти в систему от имени другого пользователя и попытаться получить доступ к ранее сохраненным файлам.

После выполнения первого ряда заданий обучающиеся должны самостоятельно сформулировать выводы об эффективности данного метода защиты.

Современные операционные системы предоставляют администраторам обширные возможности по гибкой настройке доступа пользователей к различным ресурсам компьютера. Подробное изучение всех возможностей администрирования займет очень

много времени и требует от обучающегося владения определенными навыками. Однако для организации простого ограничения доступа от обучающегося не требуется наличия специальных знаний.

На втором этапе занятия обучающимся предлагается освоить метод разграничения доступа. Данный метод позволяет ограничить доступ пользователей к файлам и папкам, находящимся на компьютере, помимо правил, которые по умолчанию формируются системой при создании профиля пользователя.

В процессе выполнения упражнения обучающиеся под руководством педагогического работника должны задать перечень пользователей и права доступа (чтение, запись, изменение и т.д.) к заранее выбранным папке или файлам. Первое, на что следует обратить внимание – все действия на данном этапе проводятся от имени администратора, а не обычного пользователя.

Для закрепления полученных знаний обучающимся предлагается поочередно войти в систему от каждого пользователя и оценить результат, пытаясь получить доступ к соответствующим папкам и файлам.

Главный вывод, который должны сделать обучающиеся по окончании данного упражнения: механизм разграничения доступа позволяет эффективно защищать данные от обычных пользователей, работающих на одном компьютере, однако он совершенно не применим против пользователей с правами администратора.

Кроме того, следует акцентировать внимание обучающихся на то, что к выбору пароля учетной записи необходимо подходить достаточно ответственно. Так, пароль должен содержать не менее 8 символов, включать в себя строчные и прописные буквы, спецсимволы и не должен быть производным от слов. Кроме того, важно отметить, что даже если за компьютером работает один пользователь, то не следует активировать функцию автоматического входа в систему, поскольку в этом случае любое лицо, включившее компьютер, получит доступ ко всем файлам и параметрам используемой учетной записи.

Для более эффективной организации защиты данных пользователей от несанкционированного доступа обучающимся предлагается освоить штатную функцию шифрования. Прежде чем приступать к выполнению практических заданий, педагогический работник должен кратко напомнить обучающимся основные принципы криптографического преобразования и указать на особую важность такого элемента, как ключ шифрования.

Для изучения штатного механизма операционной системы по шифрованию файлов и папок обучающемуся предлагается войти в систему от имени одного из пользователей, после чего в любом месте диска создать произвольный файл и в свойствах файла установить параметр шифрования. Для проверки эффективности изучаемого метода защиты

обучающимся предлагается попытаться получить доступ к зашифрованным файлам и папкам от имени другого пользователя и от имени администратора.

В процессе выполнения данного упражнения важно понимать, что при копировании файлов или при смене пароля пользователя доступ к зашифрованным данным будет невозможен без ключа шифрования. Поэтому после включения функции шифрования необходимо в обязательном порядке сохранить сформированный системой ключ, который можно дополнительно защитить паролем.

Иногда оказывается, что целостность операционной системы нарушается вследствие технического сбоя, действий вредоносных программ или злоумышленника. Формированию у обучающихся умений и навыков по восстановлению работоспособности операционной системы встроенными в нее инструментами и посвящен четвертый этап занятия.

Вначале следует акцентировать внимание обучающихся на том, что любая операционная система, какой бы совершенной она ни была, не лишена недостатков и не может обеспечить абсолютной стабильности в работе компьютера. Всегда возможно неудачное сочетание оборудования и программного обеспечения, установленного пользователем компьютера, которое может вывести из строя операционную систему [4]. Кроме того, не исключены действия самого пользователя, а также третьих лиц, в результате которых загрузка операционной системы станет невозможной. Для восстановления системы можно обратиться к соответствующим специалистам, однако на это будут потрачены дополнительные средства, а также уйдет время, что в случае если необходимая для работы пользователя информация содержится только на данном персональном компьютере, является неприемлемым.

Ввиду того что наибольшее распространение в России получила операционная система Microsoft Windows, в рамках занятия предлагается изучение средств восстановления, реализованных именно в этой операционной системе.

Для начала обучающиеся знакомятся с функционалом восстановления системы с помощью контрольных точек восстановления. Для этого им предлагается создать контрольную точку восстановления, а затем осуществить восстановление состояния компьютера на момент ее создания из-под графического интерфейса Windows. При этом следует обратить внимание обучающихся на то, что при соответствующей настройке операционная система будет создавать контрольные точки в автоматическом режиме, однако в ряде случаев пользователю целесообразно создавать их самостоятельно, например при установке или обновлении драйверов устройств, установке неизвестного программного обеспечения и т.п. Кроме того, данный метод работает лишь в случае, если операционной системе удается запуститься.

Достаточно часто в результате сбоя операционная система вовсе перестает загружаться, в связи с чем восстановление системы из-под среды Windows становится невозможным. Поэтому обучающимся необходимо изучить возможные дополнительные способы загрузки данной операционной системы. Для этого они перезагружают компьютер и активируют меню дополнительных вариантов загрузки операционной системы, после чего под руководством педагогического работника осуществляют выбор того либо иного пункта меню загрузки.

Вариант «Загрузка последней удачной конфигурации» это первое средство, которое можно порекомендовать в случае сбоя загрузки операционной системы. В этом случае загружается последняя конфигурация реестра и драйверов устройств, при которых Windows работала стабильно. Эта конфигурация не содержит компонента, который мог приводить к сбою: он будет удален при загрузке системы в последней удачной конфигурации без возможности восстановления [5]. Если данный режим не помог устранить неполадки, то следует попробовать загрузку в безопасном режиме.

В безопасном режиме загружается минимальное количество служб и драйверов, необходимое для работы Windows. Данный режим позволяет запустить функцию восстановления системы по контрольной точке, удалить программное обеспечение, установка которого могла привести к сбою, удалить драйвера устройств и т.д. Загрузка Windows в безопасном режиме также помогает определить, на каком уровне возникла проблема [6]. Следует обратить внимание обучающихся на то, что если после загрузки в безопасном режиме система работает стабильно, то причина кроется в загружаемых файлах.

Безопасный режим с поддержкой командной строки позволяет загрузить командную строку вместо стандартной графической оболочки Windows. Данный режим бывает полезен, если имеют место неполадки с запуском проводника, а также незаменим в случае блокировки графического интерфейса вредоносным программным обеспечением. При изучении данного режима следует обратить внимание обучающихся на две полезные утилиты, которые могут быть запущены из-под командной строки: CHKDSK и SFC. Первая утилита предназначена для проверки жестких дисков компьютера на ошибки файловой системы, в том числе на физические повреждения, а также их исправления. Вторая утилита представляет собой средство проверки системных файлов и позволяет пользователям проверять системные файлы на отсутствие повреждений, а также восстанавливать поврежденные системные файлы. Необходимо отметить, что данные утилиты могут быть запущены только из-под учетной записи с правами администратора.

После запуска обучающимися различных вариантов безопасного режима следует ознакомить их с возможностями среды восстановления Windows (Windows Recovery

Environment). Для этого они в меню загрузки выбирают пункт «Устранение неполадок компьютера». Данная среда содержит достаточно много инструментов, предназначенных для восстановления работоспособного состояния компьютера, включая средства для автоматического восстановления запуска, восстановления системы по контрольной точке, восстановления системы по ранее созданному образу, диагностику оперативной памяти, а также возможность запуска командной строки. Подробно рассматривать все инструменты среды восстановления в ходе занятия нецелесообразно, однако следует выделить некоторое время на каждый из них для того, чтобы у обучающихся сложилось представление о том, для каких целей предназначен каждый из этих инструментов.

В конце занятия педагогическому работнику необходимо подвести его итоги, организовав коллективное обсуждение особенностей изученных методов защиты информации штатными средствами операционной системы.

Предложенная методика проведения практического занятия позволяет обучающимся, не имеющим глубоких специальных познаний в области защиты и восстановления информации, приобрести навыки использования механизмов организации парольной защиты данных и разграничения доступа к информации, а также простейших методов шифрования и восстановления данных штатными средствами операционных систем, доступными на любом пользовательском компьютере. Данные навыки будут полезны не только специалистам, имеющим дело с конфиденциальной информацией, но и всем, кто по роду своей деятельности постоянно использует компьютерную технику.

Дополнительно стоит отметить, что при выборе инструментов для практической работы обучающихся предпочтение отдавалось штатному, предустановленному на любом компьютере программному обеспечению, которое входит в состав практически любой операционной системы. Такой выбор позволяет будущим специалистам применять полученные навыки в своей профессиональной деятельности независимо от особенностей используемого программного обеспечения.

Список литературы

1. О персональных данных: Федеральный закон от 27 июля 2006 г. № 152-ФЗ // Собрание законодательства РФ. - 2006. - N 31. - Ст. 3451.
2. Лясин Д.Н. Методы и средства защиты компьютерной информации: учеб. пособие / Д.Н. Лясин, С.Г. Саньков; ВолгГТУ, ВПИ (филиал) ВолгГТУ. - Волгоград: ВолгГТУ, 2005. - 127 с.
3. Бабикова Е.В. Применение виртуальных машин в образовании // Современные

технологии преподавания естественно-научных дисциплин в системе общего и профессионального образования: сборник материалов Международного научно-практического форума. - Борисоглебский филиал ФГБОУ ВО «Воронежский государственный университет», 2016. - С. 8-10.

4. Ланина Э.П., Шишкин М.Ю. Об устранении ошибок, возникающих на этапе загрузки ОС, при отсутствии дополнительных инструментов // Вестник Иркутского государственного технического университета. - 2013. - № 9 (80). - С. 12-17.

5. Загрузка последней удачной конфигурации Windows 7 [Электронный ресурс]. - URL: http://www.rem-tv.com/zagruzka/zagruzka-poslednej-udachnoj-konfiguracii-windows-7.html (дата обращения: 01.12.2017).

6. Изучаем безопасный режим Windows 7 [Электронный ресурс]. - URL: http://ustanovkaos.ru/reshenie-problem/bezopasnyj-rezhim-windows-7.html (дата обращения: 01.12.2017).