УДК 004.056:378

И.В. Капгер, Е.Е. Журилова, А.А. Миронова

Пермский национальный исследовательский политехнический университет,
Пермь, Россия

О РАЗРАБОТКЕ УЧЕБНО-ЛАБОРАТОРНОГО СТЕНДА ДЛЯ ИЗУЧЕНИЯ АППАРАТНОГО МОДУЛЯ ДОВЕРЕННОЙ ЗАГРУЗКИ «АККОРД»

Сформулирована актуальная проблема повышения качества практической подготовки специалистов по защите информации. Раскрыты особенности развития учебно-лабораторной базы для их обучения. Проанализирована проблема изучения средств защиты информации от несанкционированного доступа, обусловлена необходимость практической подготовки квалифицированных специалистов. Приведена структура затрат в госведомствах и корпоративных системах на информационную безопасность по классам продуктов защиты информации. Проанализированы компетенции выпускников вузов, формируемые в соответствии с ФГОС ВПО по направлению подготовки «Информационная безопасность». Приведены основные требования по защите автоматизированных систем с использованием аппаратного модуля доверенной загрузки «Аккорд» от несанкционированного доступа в соответствии с установленной классификацией. Приведено краткое описание функциональных возможностей аппаратного модуля доверенной загрузки «Аккорд». Перечислен состав программных и аппаратных средств комплекса, представлен порядок их функционирования и взаимодействия на различных этапах загрузки и дальнейшей работы. Приведена схема размещения учебно-лабораторного стенда на основе программно-аппаратного комплекса «Аккорд» в учебной лаборатории, оборудованной необходимыми для выполнения учебных задач рабочими станциями. Перечислены основные задачи, решаемые обучаемыми в процессе выполнения заданий с использованием аппаратного модуля доверенной загрузки «Аккорд». Представлена последовательность отработки обучаемыми студентами алгоритма создания нового пользователя, присвоения ему идентификатора и прав доступа. Пошаговый алгоритм выполняемых задач сопровождается необходимыми пояснениями и рисунками. Определены перспективы дальнейшего развития учебно-лабораторного стенда и использования его в учебном процессе. Проведена оценка эффективности использования учебно-лабораторного стенда на основе контроля сформированных компетенций обучаемых.

Ключевые слова: учебно-лабораторная база, программно-аппаратный комплекс, аппаратный модуль доверенной загрузки, несанкционированный доступ, техническое средство защиты информации, требования по защите информации.

I.V. Kapger, E.E. Zhurilova, A.A. Mironova

Perm National Research Polytechnic University, Perm, Russian Federation

ABOUT THE DEVELOPING OF EDUCATIONAL AND LABORATORY BENCH FOR STUDY OF HARDWARE MODULE TRUSTED BOOT «ACCORD»

It was formulated the actual problem of quality improvement of practical training to specialists in information security. It was exposed the features of development study and la-boratory facilities for their study. The problem of studying facilities to protect information from unauthorized access was analyzed, necessity of practical preparing qualificated special-ists was caused. It was analyzed the competence of graduates, which forms with accordance to GEF FPO towards training «Information Security». Shown the main requirements for pro-tection automated system with using hardware module of trusted boot «Accord» from unau-thorized access in accordance to established classification. It was listed a brief description of functional facilities of hardware module of trusted boot «Accord». Consistency of software and hardware complex, rules of its function and interact in various stages of loading and fur-ther work were listed. It was shown a scheme of placing educational and laboratory bench, which base on hard-ware and software complex «Accord», equipped with workstations which are necessary to perform the tasks. List the main tasks solving students during the execution of task using the hardware module of trusted boot «Accord». Show the sequence working out by students the algorithm creating a new user, assigning the ID and access rights. Step by step algorithm of running tasks is accompanied the neces-sary explanations and pictures. Identified the prospects of further development of teaching and laborato-ry bench and using it in the learning process. The effectiveness evaluation of using educational and laboratory bench based on the students competencies control.

Keywords: educational and laboratory facilities, software and hardware complex, hardware module of trusted boot, unauthorized access, technical tool to information security, requirements for information security.

Требования к подготовке специалистов по защите информации определены на уровне государственных стандартов. В соответствии с данными требованиями выпускник вуза должен обладать обширным перечнем универсальных знаний в разнообразных областях. Это обусловливает ряд проблем качества подготовки кадров в быстро меняющихся современных условиях.

Одной из таких проблем является недостаточная укомплектованность лабораторий учебных заведений современным программным обеспечением, средствами защиты информации, методическими материалами. Кроме того, сохраняется актуальность проблемы недостаточной практической подготовки студентов [1].

Развитие учебно-лабораторной базы для подготовки специалистов по информационной безопасности может осуществляться путем внедрения в процесс их подготовки занятий на лабораторных стендах на основе наиболее распространенных средств защиты информации [2]

или создания специализированных лабораторий для исследования защищенности различных видов автоматизированных систем от актуальных угроз безопасности информации [3].

Для совершенствования подготовки кадров на базе ПНИПУ разработан и внедрен в учебный процесс учебно-лабораторный стенд для студентов, обучающихся по направлению «Информационная безопасность» и специальности «Информационная безопасность автоматизированных систем». Данный лабораторный стенд функционирует на основе программно-аппаратного комплекса (ПАК) российского производства аппаратного модуля доверенной загрузки (АМДЗ) «Аккорд» и относится к средствам защиты информации (СЗИ) от несанкционированного доступа (НСД).

В современных условиях СЗИ данного класса довольно часто используются для защиты информации на объектах информатизации. Например, по результатам аналитического исследования, проведенного компанией «Код безопасности», еще в 2013 г. СЗИ от НСД, а также модули доверенной загрузки вошли в тройку наиболее востребованных продуктов в госведомствах и корпоративных системах (рис. 1), что обусловливает необходимость изучения порядка их установки и настройки при подготовке квалифицированных специалистов [4].

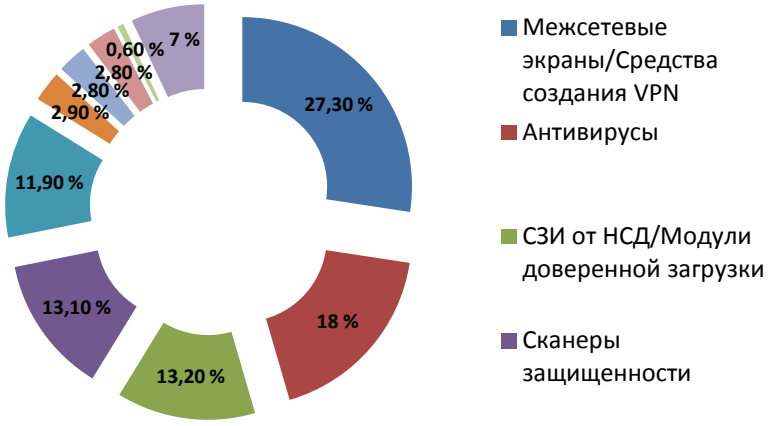

Рис. 1. Структура затрат на информационную безопасность по классам продуктов

В процессе использования учебно-лабораторного стенда предполагается формирование у студентов компетенций, определенных на основе современных требований ФГОС ВПО по направлению подготовки

«Информационная безопасность». Такими компетенциями являются способность администрировать подсистемы информационной безопасности объекта, а также способность выполнять работы по установке, настройке и обслуживанию технических и аппаратно-программных средств защиты информации [5].

АМДЗ «Аккорд» может быть эффективно применен для построения систем защиты информации от НСД в соответствии с руководящими документами ФСТЭК России. При этом сам комплекс удовлетворяет требованиям по защите информации по классу защищенности «1Д», а в качестве средства идентификации и аутентификации пользователей и контроля целостности программной среды может быть использован при создании автоматизированных систем (АС) до класса «1Б» включительно. При необходимости построения полноценной системы защиты информации дополнительно к комплексу СЗИ от НСД АМДЗ «Аккорд» устанавливается специальное программное обеспечения «Аккорд-Win32» или «Аккорд-Win64», предназначенное для работы в ОС семейства Windows.

Комплекс СЗИ от НСД АМДЗ «Аккорд» представляет собой АМДЗ для IBM-совместимых ПК – серверов и рабочих станций, обеспечивающий, в первую очередь, доверенную загрузку операционных систем, а также идентификацию, аутентификацию пользователей, контроль целостности файлов и аппаратного обеспечения ПК при загрузке. Как правило, под термином «доверенная загрузка» понимается загрузка различных операционных систем (ОС) только после проведения контрольных процедур идентификации и аутентификации пользователя, а также проверки целостности технических и программных средств ПЭВМ [6].

В соответствии с методическими рекомендациями ФСТЭК России доверенная загрузка – это загрузка операционной системы средства вычислительной техники с заранее определенных постоянных машинных носителей при обязательном успешном прохождении процедур проверки целостности программной и аппаратной среды и идентификации и аутентификации [7].

Комплекс начинает работу сразу после выполнения системного кода BIOS – до загрузки операционной системы и обеспечивает доверенную загрузку ОС, использующих одну из поддерживаемых файловых систем. Это, в частности, ОС типа MS-DOS, ОС семейства Windows, QNX, OS/2, UNIX, LINUX,BSD и др. [8].

Значительное количество инцидентов информационной безопасности возникает по причине уязвимости сервисов операционной системы и приложений, что обусловливает необходимость поддержки в системе защиты информации дополнительных средств доверенной загрузки. Так, больше половины опрошенных компаний (52 %) столкнулись в 2015 г. с инцидентами в области информационной безопасности [9], существенная часть которых обусловлена данным фактором.

Комплекс СЗИ от НСД АМДЗ «Аккорд» включает в себя программные и аппаратные средства. Их функционирование и взаимодействие на различных этапах загрузки/работы представлены на рис. 2.

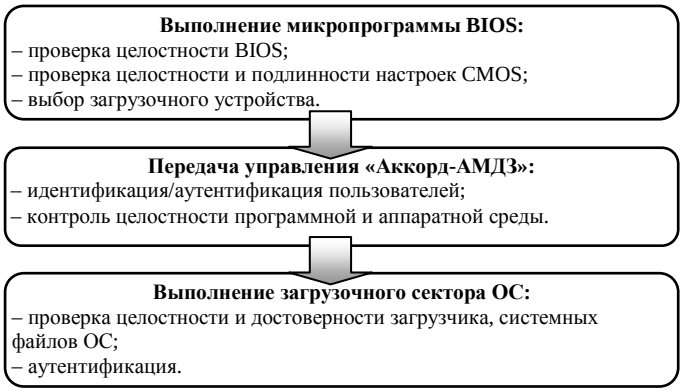

Рис. 2. Этапы доверенной загрузки комплекса «Аккорд»

Учебно-лабораторный стенд на основе ПАК АМДЗ «Аккорд» размещен в лаборатории, оборудованной необходимыми для выполнения учебных задач рабочими станциями. Схема размещения оборудования учебно-лабораторного стенда приведена на рис. 3.

В процессе выполнения заданий с использованием АМДЗ «Аккорд» обучаемыми решаются следующие учебные задачи:

– изучение особенностей идентификации пользователей при использовании персонального идентификатора в виде электронного ключа;

– изучение способов загрузки операционной системы со съемных носителей, а также способов блокировки такой загрузки;

– изучение критериев проверки контроля целостности, способов обеспечения контроля целостности технических средств и программных средств;

– изучение способов обеспечения доверенного режима загрузки операционных систем с различными типами файловых систем.

При этом каждая из перечисленных выше учебных задач может быть детализирована на несколько подзадач.

Наиболее часто выполняемыми действиями при администрировании и настройке АМДЗ «Аккорд» являются отработка алгоритма создания нового пользователя и присвоение ему идентификатора. Необходимо учесть, что при первой загрузке в системе не существует зарегистрированных пользователей, поэтому из перечисленных пунктов меню существует возможность выбора только между двумя действиями – это «Администрирование» и «Выход» [10].

Выбор пункта «Администрирование» позволяет загрузить главное меню администратора. Меню предоставляет возможность работы со списком пользователей, создания дополнительных настроек и помощи. Существуют также функции работы со списком целостности и с журналом регистрации, но в связи с отсутствием зарегистрированных пользователей на начальном этапе они не активны.

Для отработки учебной задачи по созданию пользователя, назначению ему идентификатора и прав доступа необходимо выполнение следующей последовательности.

1. Выбрать команду «Пользователи» в представленном меню. Открыть список зарезервированных групп с привилегиями (рис. 3).

Рис. 3. Список зарезервированных групп и пользователей

При этом все привилегии, настроенные для группы, будут наследоваться и каждым участником этой группы, если не будет произведено отдельных настроек. Изначально настраивается учетная запись

главного администратора, которому в последующем будут доступны все функции администрирования.

2. Используя стрелки выбрать поле «Главный администратор», нажатием «Enter» отрыть окно настроек. В строках «Идентификатор» и «Пароль» вместо начального значения «нет» присвоить им значения для администратора.

3. Выбрать поле «Идентификатор» и в появившемся свободном окне с информацией об идентификаторе нажать «Новый».

4. Убедиться в появлении окна запроса идентификатора (рис. 4) и приложить к считывателю идентификатор, который присвоен главному администратору.

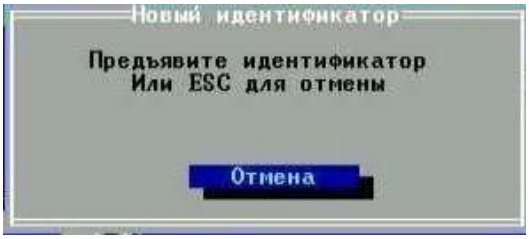

Рис. 4. Окно запроса идентификатора

5. Записать в память идентификатора секретный ключ, уникальный для каждого идентификатора. Поскольку наш идентификатор пустой, то необходимо выбрать опцию «Новый».

Для рационального использования ключей учетная запись главного администратора может быть на всех рабочих станциях одинаковой, поэтому при ее настройке на других местах, при назначении секретного ключа администратора, необходимо выбрать опцию «Существующий» (рис. 5).

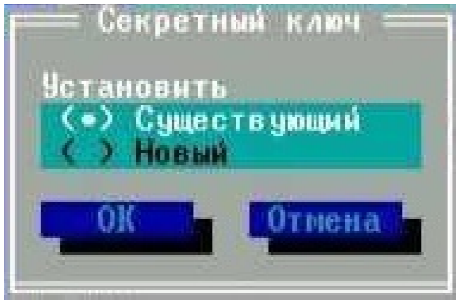

Рис. 5. Процедура добавления
секретного ключа

6. Для создания пароля к учетной записи возвратиться к окну настроек и выбрать поле «Пароль». При этом предоставляется возможность выбора генерации пароля автоматически либо создание его пользователем (рис. 6).

7. Параметры учетной записи настроены, для их применения и сохранения необходимо нажать на строку «Запись». Учетная запись главного администратора создана.

Для создания учетных записей других администраторов и пользователей можно продолжить работу в данном окне либо перезагрузить рабочую станцию и создать пользователей, используя учетную запись главного администратора.

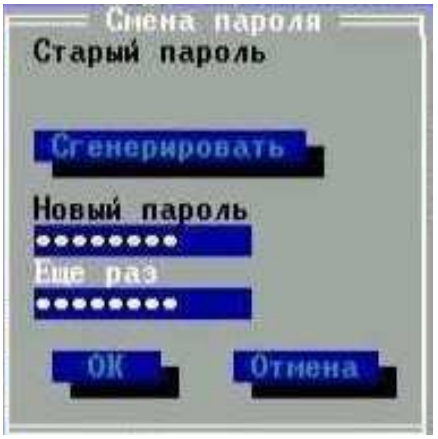

Рис. 6. Процедура установки пароля

Дальнейшая работа на учебно-лабораторном стенде АМДЗ «Аккорд» позволила учащимся получить навыки работы с ключами при проведении аутентификации, идентификации пользователей, навыки создания пользователей, групп пользователей в ПАК АМДЗ «Аккорд», а также отработать учебные задания по назначению привилегии в соответствии с необходимым уровнем доступа.

По результатам опытной эксплуатации учебно-лабораторного стенда на базе АМДЗ «Аккорд» и в процессе практических занятий была проведена оценка эффективности его работы на основе контроля сформированных компетенций обучаемых.

Таким образом, необходимость качественной подготовки специалистов по защите информации и возрастающие требования к их компетентности обусловливает потребность в совершенствовании учебно-

лабораторной базы. Внедрение в учебный процесс лабораторного стенда АМДЗ «Аккорд» позволит повысить эффективность подготовки выпускников, что крайне необходимо в настоящие дни. Владение навыками практической работы со средствами защиты от НСД повысит конкурентоспособность выпускников на рынке труда, обеспечит качество защиты корпоративных информационных систем от актуальных угроз безопасности информации.

Библиографический список

1. Миронова А.А., Шабуров А.С., Модель разработки учебно-лабораторного комплекса для подготовки специалистов по защите информации // Вестник УрФО. Безопасность в информационной сфере. Челябинск: Изд-во ЮУрГУ, 2015. – № 3(17). – С. 54–59.

2. Шабуров А.С. О разработке учебно-лабораторного стенда для построения систем защиты информации на основе АПКШ «Континент» // Научные исследования и инновации. – Пермь: Изд-во Перм. нац. исслед. политехн. ун-та, 2012. – Т. 6. – № 1–4.

3. Южаков А.А., Шабуров А.С., Рашевский Р.Б. О разработке учебно-лабораторного комплекса для исследования защищенности критически важных объектов // Вестник УрФО. Безопасность в информационной сфере. – 2012. – С. 54–59.

4. Затраты госведомств России на информационную безопасность в 2013 году [Электронный ресурс]. – URL: http://www.securitycode.ru/_upload/editor_files/otchet_po_zakupkam_goso rganov_2013.pdf (дата обращения: 28.01.2016).

5. Приказ от 28 октября 2009 г. N 496 «Об утверждении и введении в действие федерального государственного образовательного стандарта высшего профессионального образования по направлению подготовки 090900 Информационная безопасность (квалификация (степень) «Бакалавр»)» (Ред. от 31.05.2011) / Мин-во образ. и науки РФ. – М., 2009.

6. Средства защиты от несанкционированного доступа к информации [Электронный ресурс]. – URL: http://www.cnews.ru/reviews/free/oldcom/security/sapr_products.shtml (дата обращения: 13.02. 2016).

7. Меры защиты информации в государственных информационных системах. Методический документ (утв. ФСТЭК от 11 февраля 2014 г.). – М., 2014.

8. Программно-аппаратный комплекс защиты информации от НСД для ПЭВМ (РС) «Аккорд-АМДЗ» (Аппаратный модуль доверенной загрузки). Описание применения. – М., 2014.

9. Итоги исследований 2015 года в области информационной безопасности [Электронный ресурс]. – URL: http://dlp.searchinform.ru/itogi-goda-infographic/?utm_source=newsletter&utm_medium=email&utm__campaign=itogi_goda_v_oblasti_informacionnoy_bezopasnosti (дата обращения: 13.02.2016).

10. Программно-аппаратный комплекс защиты информации от НСД для ПЭВМ (РС) «Аккорд-АМДЗ» (Аппаратный модуль доверенной загрузки). Руководство администратора. – М., 2014.

References

1. Mironova A.A., Shaburov A.S., Model' razrabotki uchebno-laboratornogo kompleksa dlia podgotovki spetsialistov po zashchite informatsii [The development model of teaching and laboratory-complex for information security specialists training]. *Vestnik Ural'skogo federal'nogo okruga. Bezopasnost' v informatsionnoi sfere*. Chelyabinsk: Iuzhno-Ural'skii gosudarstvennyi universitet, 2015, no. 3(17), pp. 54-59.

2. Shaburov A.S. O razrabotke uchebno-laboratornogo stenda dlia postroeniia sistem zashchity informatsii na osnove APKSh «Kontinent» [On the development of educational and laboratory-bench for data protection systems design based on hardware and software encrypting complex "Continent".Research and innovation]. *Nauchnye issledovaniia i innovatsii*. Permskii natsional'nyi issledovatel'skii politekhnicheskii universitet, 2012, vol. 6, no. 1–4.

3. Iuzhakov A.A., Shaburov A.S., Rashevskii R.B. O razrabotke uchebno-laboratornogo kompleksa dlia issledovaniia zashchishchennosti kriticheski vazhnykh ob"ektov [On the educational and laboratory-complex development for mission-critical obejects security research]. *Vestnik Ural'skogo federal'nogo okruga. Bezopasnost' v informatsionnoi sfere*, 2012, pp. 54-59.

4. Iuzhakov A.A., Shaburov A.S., Rashevskii R.B. O razrabotke uchebno-laboratornogo kompleksa dlia issledovaniia zashchishchennosti kriticheski vazhnykh ob"ektov [Information security expenses of Russian

state structures in 2013], available at: http://www.securitycode.ru/_upload/editor_files/otchet_po_zakupkam_gosorganov_2013.pdf (accessed 28 January 2016).

5. Prikaz ot 28 October 2009 goda № 496 "Ob utverzhdenii i vvedenii v deistvie federal'nogo gosudarstvennogo obrazovatel'nogo standarta vysshego professional'nogo obrazovaniia po napravleniiu podgotovki 090900 informatsionnaia bezopasnost' (kvalifikatsiia (stepen') “Bakalavr”)" [Ministry of Education and Science of the Russian Federation.Order 496n of October 28, 2009 "On approval and en-actment of the federal state educational standards of higher education in the direction of preparation 090900 Information Security (qualification (degree) "Bachelor")"]. *Ministerstvo obrazovaniia i nauki Rossiiskoi Federatsii*. Moscow, 2009.

6. Sredstva zashchity ot nesanktsionirovannogo dostupa k informatsii [Means of unauthorized access data protection], available at: http://www.cnews.ru/reviews/free/oldcom/security/sapr_products.shtml (accessed 13 February 2016).

7. Mery zashchity informatsii v gosudarstvennykh informatsionnykh sistemakh. Metodicheskii dokument. Utverzhden FSTEK ot 11 February 2014 goda [Information security measures in state information systems. Methodological document FSTEC dd. February 11, 2014]. Moscow, 2014.

8. Programmno-apparatnyi kompleks zashchity informatsii ot NSD dlia PEVM (RS) "Akkord-AMDZ" (Apparatnyi modul' doveren-noi zagruzki). Opisanie primeneniia [Hardware-software complex for information protection from unauthorized access to PC. "Accord-TLHM" (trusted load hardware module). Use description]. Moscow, 2014.

9. Itogi issledovanii 2015 goda v oblasti informatsionnoi bezopasnosti [Results in the field of information security research in 2015], available at: http://dlp.searchinform.ru/itogi-goda-infographic/?utm_source=newsletter& utm_medium=email&utm_campaign=itogi_goda_v_oblasti_informacionnoy_bezopasnosti (accessed 13 February 2016).

10. Programmno-apparatnyi kompleks zashchity informatsii ot NSD dlia PEVM (RS) «Akkord-AMDZ» (Apparatnyi modul' doverennoi zagruzki). Rukovodstvo administratora [Hardware-software complex information protection from unauthorized access to PC (RS) "Accord-TLHM" (trusted load hardware module).Administrator manual]. Moscow, 2014.

Сведения об авторах

Капгер Игорь Владимирович (Пермь, Россия) – кандидат технических наук, доцент кафедры автоматики и телемеханики Пермского национального исследовательского политехнического университета, начальник отдела информационной безопасности Пермской печатной фабрики – филиала ФГУП «Гознак» (614990, г. Пермь, шоссе Космонавтов, 115, e-mail: kapger@mail.ru).

Журилова Елена Евгеньевна (Пермь, Россия) – студентка Пермского национального исследовательского политехнического университета (614990, Пермь, Комсомольский пр., 29, e-mail: ele11485995@yandex.ru).

Миронова Анна Алексеевна (Пермь, Россия) – студентка Пермского национального исследовательского политехнического университета (614990, Пермь, Комсомольский пр., 29, e-mail: mir550@yandex.ru).

About the authors

Kapger Igor Vladimirovich, (Perm, Russian Federation) is a Ph.D. in Technical Sciences, Associate Professor of the Department of Automation and Telemechanics Perm National Research Polytechnic University, Head of Information Security Department of the Perm Printing Factory – branch of Federal State Unitary Enterprise “Goznak” (614990, Perm, 115, Kosmonavtov Highway, e-mail: kapger@mail.ru).

Zhurilova Elena Evgen’evna (Perm, Russian Federation) is a Student Perm National Research Polytechnic University (614990, Perm, 29, Komsomolsky pr., e-mail: ele11485995@yandex.ru).

Mironova Anna Alekseevna (Perm, Russian Federation) is a Student Perm National Research Polytechnic University (614990, Perm, 29, Komsomolsky pr., e-mail: mir550@yandex.ru).

Получено 20.02.2016