УДК 004.056:378

А.С. Шабуров, А.А. Миронова

Пермский национальный исследовательский политехнический университет,
Пермь, Россия

О РАЗРАБОТКЕ УЧЕБНО-ЛАБОРАТОРНОГО СТЕНДА ДЛЯ ПОСТРОЕНИЯ СИСТЕМ ЗАЩИТЫ ИНФОРМАЦИИ НА ОСНОВЕ УСТРОЙСТВА КРИПТОГРАФИЧЕСКОЙ ЗАЩИТЫ ДАННЫХ «КРИПТОН»

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. Проанализированы компетенции выпускников вузов, формируемые в соответствии с ФГОС ВО по направлению подготовки 10.03.01 «Информационная безопасность» и специальности 10.05.01 «Информационная безопасность автоматизированных систем». В настоящей статье предлагается краткое описание функциональных возможностей аппаратно-программного комплекса защиты данных «Криптон». Представлены отличительные особенности устройства криптографической защиты данных (УКЗД) серии «Криптон», программное обеспечение которого позволяет решить некоторые типовые задачи по защите информации. Приведен состав устройства криптографической защиты данных серии «Криптон» в зависимости от его комплектации. Также описан процесс разработки учебно-лабораторного стенда для изучения, построения и исследования систем защиты информации на основе криптографических систем шифрования. Приведен пример выполнения лабораторного задания по организации криптографической сети с использованием устройства криптографической защиты данных «Криптон», с указанием цели работы, порядка работы, с наличием теоретического введения, практической части и контрольных вопросов. Теоретическое введение содержит такие основные понятия, как криптографическая сеть, сетевой ключ, сетевая таблица, сетевой набор, организация криптографической сети, шифрование файлов для передачи в криптографической сети, настройка параметров. Разработанный учебно-лабораторный стенд позволяет применять его в программе подготовки студентов по направлению «Информационная безопасность» и специальности «Информационная безопасность автоматизированных систем», а также использовать его для реализации программ дополнительного профессионального образования и повышения квалификации специалистов по защите информации.

Ключевые слова: информационная безопасность, учебно-лабораторный стенд, система защиты информации, криптография, устройство криптографической защиты данных, шифрпроцессор, открытый канал связи.

A.S. Shaburov, A.A. Mironova

Perm National Research Polytechnic University, Perm, Russian Federation

ON THE DEVELOPMENT OF THE EDUCATIONAL-LABORATORY STAND FOR THE BUILDING OF INFORMATION SECURITY SYSTEMS BASED ON THE CRYPTOGRAPHIC SECURITY DATA DEVICE «CRYPTON»

The urgent issue of the quality increasing of specialists in information security training has been formulated. The features of development of educational-laboratory facilities useful for specialists have been revealed. The problem of security information means against unauthorized access has been analyzed; the necessity of skilled specialists training has been stipulated. The competences of graduated students in universities, based in compliance with FSES (Federal State Educational Standard) in the course 10.03.01 «Information security» and 10.05.01 «Information security of automatized systems». The current article offers a brief description of functional opportunities of information security computer appliance «Crypton». The distinctive features of the cryptographic security data device «Crypton», which software allows solving certain routine problems, have been introduced. The structure of a cryptographic security data device «Crypton» according to its kitting-up has been stated. The process of development of the educational-laboratory stand for the study, construction and research of information security systems based on the cryptographic encryption systems has been described. The execution example of a laboratory work on the organization of cryptographic network, which is based on the he cryptographic security data device «Crypton» and contains the goal of the work, the order, theoretical introduction, practical work and control questions, has been given. Theoretical introduction contains such basic notions as cryptographic network, settings, network key, network table, network kit, organization of cryptographic network, files encryption for transmission in the cryptographic network, settings. The developed educational-laboratory stand allows to apply it in the training course of students studying «Information security», «Information security of automatized systems» as well as to use it for the realization of additional professional education programs and for advanced training of information security specialists.

Keywords: information security, educational-laboratory stand, information security system, cryptography, cryptographic security data device, cryptographic processor, open communication channel.

Развитие учебно-лабораторной базы для подготовки специалистов по защите информации, оперативная адаптация лабораторных и практических занятий для изучения наиболее актуальных вопросов информационной безопасности являются задачами совершенствования системы подготовки кадров. Поиск путей совершенствования методических подходов в образовательной деятельности как в целом, так и в практической составляющей обучения является одной из важнейших задач высшей школы на современном этапе [1].

Модернизация лабораторной базы для подготовки специалистов по защите информации предполагает создание новых учебно-лабораторных комплексов для исследования защищенности информационных систем, что позволит сформировать необходимые практические навыки и выра-

ботать требуемые компетенции для будущей профессиональной деятельности студентов. Особенно важно формирование высокого уровня компетенций при подготовке к эксплуатации критически важных систем и объектов [2].

В соответствии с современными требованиями ФГОС ВО по направлению подготовки «Информационная безопасность» выпускник вуза должен быть подготовлен для выполнения комплекса работ по установке, настройке и обслуживанию программных, программно-аппаратных (в том числе криптографических) и технических средств защиты информации[*]. Аналогичные требования предъявляются и к специалистам, подготовленным для защиты информации в автоматизированных системах[**].

В ходе обучения немаловажное значение приобретает способность уяснять закономерности функционирования и особенности применения подобных средств, поскольку совершенствование процессов обработки информации влечет за собой неизбежное развитие средств и методов обеспечения информационной безопасности. Очевидно, в условиях лабораторного исследования при ограничениях учебного времени студент должен овладеть методологией построения систем защиты информации в текущем периоде и на перспективу [3, 4].

Выполнение практических задач на основе интегрированных в учебный процесс учебно-лабораторных комплексов в первую очередь предполагает приобретение умений и навыков работы по эксплуатации средств защиты информации. Учебные задачи планируются как для отдельных автоматизированных рабочих мест [5], изучения специализированных, в том числе криптографических средств защиты [6], так и при внедрении комплексных решений по информационной безопасности [7, 8].

Получение практических навыков при изучении средств защиты информации, в свою очередь, позволяет развивать различные научные направления в области обеспечения информационной безопасности [9, 10],

[*] Федеральный государственный образовательный стандарт высшего образования по направлению подготовки 10.03.01 Информационная безопасность (уровень бакалавриата) (утв. приказом Мин-ва обр. и науки РФ от 1 декабря 2016 г. № 1515 // Доступ из справ.-правовой системы КонсультантПлюс.

[**] Федеральный государственный образовательный стандарт высшего образования по спец. 10.05.03 «Информационная безопасность автоматизированных систем (уровень специалитета)», (утв. приказом Мин-ва обр. и науки РФ от 1 декабря 2016 г. № 1509 // Доступ из справ.-правовой системы КонсультантПлюс.

исследовать проблемы безопасности информации как с точки зрения актуальности отдельных типов угроз [11], так и внедрения инновационных решений для защиты сложных технических систем и объектов [12].

Современный рынок постоянно пополняется более совершенными разновидностями и модификациями сертифицированных средств защиты информации, как правило, обладающими стандартными, унифицированными требованиями [13]. Это обусловливает необходимость изучения общих принципов и типовых задач их применения. Примером серии подобных и наиболее распространенных средств защиты являются устройства криптографической защиты данных (УКЗД) серии «Криптон». Это аппаратные шифраторы для PC-совместимых компьютеров, применяемые в составе средств и систем криптографической защиты для обеспечения информационной безопасности (в том числе защиты с высоким уровнем секретности) в государственных и коммерческих структурах. Они гарантируют защиту информации, обрабатываемой на персональном компьютере, передаваемой по открытым каналам связи, и предназначены для обеспечения защиты различных видов конфиденциальной информации[***].

Отличительные особенности УКЗД серии «Криптон»:

– аппаратная реализация алгоритма криптографического преобразования гарантирует целостность алгоритма;

– шифрование производится, и ключи шифрования хранятся в самой плате, а не в оперативной памяти компьютера;

– есть аппаратный датчик случайных чисел;

– загрузка ключей шифрования в устройство «Криптон» со смарт-карт и идентификаторов Touch Memory (i-Button) производится напрямую, минуя ОЗУ и системную шину компьютера, что исключает возможность перехвата ключей;

– на базе устройств «Криптон» можно создавать системы защиты информации от несанкционированного доступа и разграничения доступа к компьютеру;

[***] Методические рекомендации по разработке нормативных правовых актов, определяющих угрозы безопасности персональных данных, актуальные при обработке персональных данных в информационных системах персональных данных, эксплуатируемых при осуществлении соответствующих видов деятельности. Утверждены руководством 8 Центра ФСБ России от 31 марта 2015 года № 149/7/2/6-432. Доступ из справ.-правовой системы КонсультантПлюс.

– применение специализированного шифрпроцессора для выполнения криптографических преобразований разгружает центральный процессор компьютера;

– возможна также установка на одном компьютере нескольких устройств «Криптон», что еще более повысит скорость шифрования (для устройств с шиной PCI);

– использование парафазных шин в архитектуре шифрпроцессора исключает угрозу снятия ключевой информации по возникающим в ходе криптографических преобразований колебаниям электромагнитного излучения в цепях «земля – питание» микросхемы.

УКЗД серии «Криптон» независимо от операционной среды обеспечивают защиту ключей шифрования и неизменность алгоритма шифрования. Вся используемая в системе ключевая информация может шифроваться на мастер-ключах и храниться на внешнем носителе в зашифрованном виде, т.е. появляться и использоваться в расшифрованном виде только внутри системной области УКЗД.

Помимо перечисленных выше функций УКЗД «Криптон» может обладать дополнительными свойствами, незаменимыми при построении различных систем защиты от НСД на базе данного устройства, к которым относятся:

– функция электронного замка персонального компьютера;

– наличие энергонезависимой памяти для хранения журнала операций и файл-списка (списка файлов операционной системы, целостность которых необходимо проверять до загрузки ОС, с рассчитанными для них контрольными значениями) [14].

Программное обеспечение устройств «Криптон» позволяет решать следующие типовые задачи:

– шифровать компьютерную информацию (файлы, группы файлов и разделы дисков), обеспечивая их конфиденциальность;

– осуществлять электронную цифровую подпись файлов, проверяя их целостность и авторство;

– создавать прозрачно-шифруемые логические диски, максимально облегчая и упрощая работу пользователя с конфиденциальной информацией;

– формировать криптографически защищенные виртуальные сети, шифровать IP-трафик и обеспечивать защищенный доступ к ресурсам сети мобильных и удаленных пользователей;

– создавать системы защиты информации от несанкционированного доступа и разграничения доступа к компьютеру.

В состав УКЗД «Криптон» в зависимости от комплектации могут быть включены:

– контроллеры смарт-карт;

– системы защиты информации от несанкционированного доступа (СЗИ НСД);

– программы абонентского шифрования, электронной подписи и защиты электронной почты;

– коммуникационные программы прозрачного шифрования IP-пакетов и ограничения доступа к компьютеру по сети;

– криптомаршрутизаторы;

– библиотеки поддержки различных типов смарт-карт;

– библиотеки функций шифрования и электронной цифровой подписи для различных операционных систем [15].

Учебно-лабораторный стенд размещен в специализированной лаборатории кафедры автоматики и телемеханики, оборудованной необходимыми для выполнения учебных задач персональными компьютерами.

Пример выполнения лабораторного задания по организации криптографической сети с использованием УКЗД «Криптон» может быть представлен следующим образом.

1. *Цель работы.* Изучить возможности использования пакета «Криптон». Шифрование для организации криптографической сети обмена электронными документами. Получить представление о задачах, возлагаемых на администратора и пользователей криптографической сети.

2. *Порядок работы*. Последовательно, в течение отведенного расписанием занятий времени, отработать следующие вопросы:

– изучить теоретический материал;

– оформить конспект к работе, получить допуск к выполнению работы;

– выполнить упражнения из практической части работы;

– оформить отчет по лабораторной работе и защитить его.

3. *Теоретические сведения. Криптографическая сеть.* Множество компьютеров, называемых узлами, между которыми тем или иным способом осуществляется направленный обмен зашифрованной информа-

цией, называется криптографической сетью. Направленный обмен подразумевает возможность зашифровать передаваемую информацию таким образом, чтобы расшифровать ее мог только тот узел, для которого она предназначалась. Обмен информацией между узлами криптографической сети может осуществляться как посредством локальных и глобальных сетей, так и с помощью сменных носителей. В пакете «Криптон» шифрование для защиты данных в криптографической сети используется симметричный алгоритм шифрования – ГОСТ 28147-89.

Сетевой ключ. Секретный ключ используется для зашифрования файлов с целью передачи их между узлами криптографической сети. Все узлы сети нумеруются. Для каждого узла, с которым планируется обмен информацией, необходимо иметь свой сетевой ключ. Задача обеспечения сетевыми ключами возлагается на администратора сети. Сетевые ключи хранятся в Сетевом наборе.

Сетевая таблица. Для обмена зашифрованной информацией между N узлами необходимо $N\cdot(N-1)$ ключей (каждый с каждым). Фактически это таблица, где в заголовках строк и столбцов проставлены номера узлов, а в ячейках хранятся ключи. Эта матрица симметрична, т.е. ключ для передачи от узла А узлу Б (сетевой ключ А–Б) в точности равен сетевому ключу Б–А. Сетевая таблица при создании зашифровывается на Ключе сетевой таблицы (КСТ).

Сетевой набор. Из полной Сетевой таблицы необходимо для каждого из узлов сформировать набор ключей для связи с другими узлами. Фактически такой набор представляет собой одну из строк таблицы. Сетевой набор хранится в файле NNNNN.SYS в каталоге сетевых ключей, где NNNNN – пятизначный десятичный номер данного узла. Он всегда зашифрован на Ключе сетевого набора (КСН), хранящемся в файле NNNNN.KEY в каталоге сетевых ключей. КСН получают вместе с Сетевым набором от администратора криптографической сети. При получении КСН обычно зашифрован на главном ключе, поэтому рекомендуется перешифровать его на пароле.

Организация криптографической сети. Для организации криптографической сети администратор должен выполнить следующие действия:

1. Создать Сетевую таблицу. Для этого необходимо указать количество узлов криптографической сети и имя Сетевой таблицы.

В результате автоматически создается новый Ключ Сетевой таблицы NET_SYS.KEY, на котором автоматически зашифровывается Сетевая таблица KEY_NET.SYS.

2. Создать Сетевые наборы (СН) для узлов криптографической сети. По умолчанию создаются СН для всех узлов, и в каждом сетевом наборе все узлы являются доступными. При необходимости можно создать такие СН, чтобы узел мог шифровать данные только для ограниченного множества узлов криптографической сети. В результате получается множество Ключей сетевого набора (NNNNN.KEY) и Сетевых наборов (NNNNN.SYS) для узлов криптографической сети.

3. Каждому узлу присвоить свой номер NNNNN. Распределить Ключи сетевого набора и Сетевые наборы по соответствующим узлам криптографической сети. Узлу с номером NNNNN необходимо передать два файла: NNNNN.KEY и NNNNN.SYS.

Шифрование файлов для передачи в криптографической сети. Файл данных, передаваемый узлом А узлу Б, зашифровывается на Файловом (сеансовом) ключе. Файловый ключ создается автоматически при зашифровании файла данных и передается вместе с ним. Поскольку Файловый ключ не может передаваться в открытом виде, то он зашифровывается на Сетевом ключе А–Б. Этот ключ узел А берет из своего Сетевого набора.

Сетевой набор узла А зашифрован на Ключе сетевого набора (КСН) узла А, который, в свою очередь, тоже может быть зашифрован на каких-либо ключах узла А (как правило, ГК).

Узел Б по информации, присовокупленной к зашифрованному файлу, понимает, что файл пришел от узла А. Используя свои ключи, узел Б расшифровывает свой КСН.

Затем, используя КСН, узел Б расшифровывает свой набор и извлекает из него Сетевой ключ А–Б. Так как этот Сетевой ключ совпадает с тем Сетевым ключом, который использовал узел А для зашифрования, то узел Б может расшифровать Файловый ключ, пришедший вместе с файлом. Наконец, с помощью Файлового ключа расшифровывается сам файл.

Настройка параметров. После запуска Мастера ключей шифрования и выбора настройки параметров (рисунок) правая сторона панели содержит следующие настраиваемые параметры:

– «Каталог Ключей пользователя».

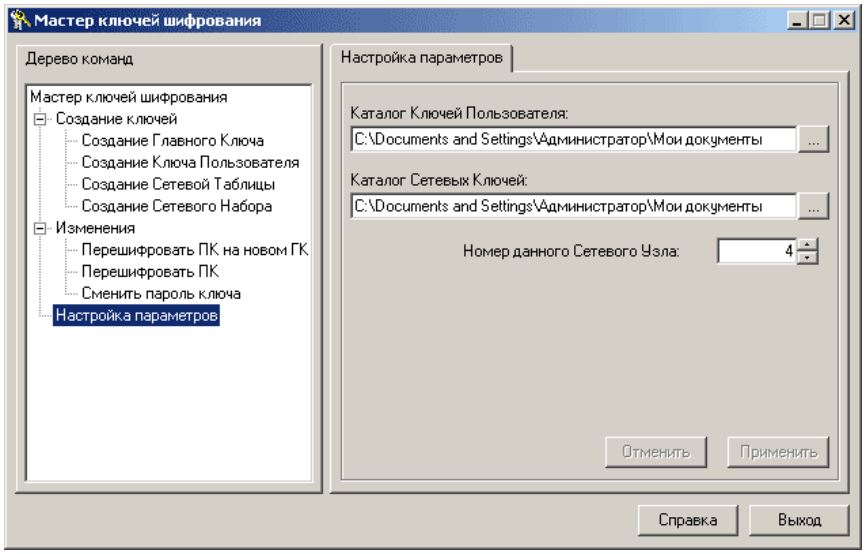

Рис. Мастер ключей шифрования УЗКД «Криптон»

Ввести каталог Ключей пользователя. В этом каталоге будет производиться поиск Ключей пользователя в следующих ситуациях:

– зашифрование файла на Ключе пользователя;

– расшифрование файла, зашифрованного на Ключе пользователя;

– перешифрование файла, зашифрованного на Ключе пользователя.

Требуемый каталог можно указать также с помощью кнопки обзора каталогов. По данной кнопке на экран выводится меню «Диски»/«Карточки», позволяющее указать каталог с помощью стандартного диалога Windows или диалога выбора устройств SCApi.

– «Каталог Сетевых ключей»

Ввести каталог Сетевых ключей. В этом каталоге будет производиться поиск Сетевых ключей в следующих ситуациях:

– зашифрование файла на Сетевом ключе;

– расшифрование файла, зашифрованного на Сетевом ключе;

– перешифрование файла, зашифрованного на Сетевом ключе.

Требуемый каталог можно указать также с помощью кнопки обзора каталогов, по которой вызывается стандартный диалог обзора папок Windows. Сетевые ключи хранятся в Сетевых наборах в файлах NNNNN.sys, где NNNNN – номер данного сетевого узла (см. раздел «Создать Сетевой набор»):

– «Номер данного сетевого узла».

Ввести номер сетевого узла – целое число в диапазоне от 1 до 30 000, идентифицирующее данный сетевой узел (пользователя или компьютер – в зависимости от организационных решений).

Для ввода в действие сделанных изменений в конфигурации следует нажать кнопку «Применить». Конфигурация будет изменена.

Для отмены внесенных изменений следует нажать кнопку «Отменить».

Параметры сохраняются в системном реестре Windows.

4. *Практическая часть*

1. Создать отдельную папку Lab5. В ней создать следующие папки:
- Key_net – для Ключа СТ и самой СТ;
- 00001, 00002, 00003, 00004 – для Ключей СН и самих СН;
- Source – для тестовых файлов и их зашифрованных вариантов.

2. Создать Сетевую таблицу для четырех узлов в каталоге Key_net.

3. Создать Сетевые наборы для всех узлов. Разложить полученные ключи СН и сами СН по соответствующим папкам 00001,…,00004.

4. Установить номер своего узла, равный 2, и указать в параметрах соответствующий каталог сетевых ключей.

5. Зашифровать тестовые файлы для узла 3.

6. Установить номер своего узла, равный 3, и указать в параметрах соответствующий каталог сетевых ключей.

7. Расшифровать тестовые файлы с автоматическим переименованием и затем полученные файлы уничтожить.

8. Установить номер своего узла, равный 1, и указать в параметрах соответствующий каталог сетевых ключей.

9. Расшифровать тестовые файлы (зашифрованные для узла 3) с автоматическим переименованием.

10. Оформить отчет о проделанных шагах 2–9, в который включить краткое описание результатов каждого шага (например, создана сетевая таблица для четырех узлов и т.д.).

11. Из папки Материалы для данной лабораторной работы в папку Lab5 скопировать Ключ СН и сам СН, соответствующий номеру варианта.

12. Установить номер своего узла, соответствующий номеру варианта, и указать в параметрах каталог сетевых ключей Lab5.

13. Зашифровать тестовые файлы для узла 11.

14. Полученные зашифрованные файлы предоставить для проверки.

5. *Контрольные вопросы*

1. Дать понятия сетевого набора и сетевой таблицы.

2. Особенности защиты данных в криптографической сети с помощью симметричных и асимметричных алгоритмов шифрования

3. Назначение Сетевых ключей и Ключей сетевых наборов.

4. Параметры, настраиваемые в пакете «Криптон» Шифрование, для работы в криптографической сети.

5. Процесс обмена зашифрованными файлами в криптографической сети.

6. Создание сетевых наборов для ограниченного числа узлов криптографической сети.

Таким образом, степень внедрения разработанного учебно-лабораторного стенда позволяет применять его в программе подготовки студентов по направлению «Информационная безопасность» и специальности «Обеспечение информационной безопасности автоматизированных систем», а также использовать его для повышения квалификации специалистов по защите информации в рамках программ дополнительного профессионального образования. Эффективность применения разработанного учебно-лабораторного стенда на основе УКЗД серии «Криптон» подтверждается приобретением требуемых компетенций, а также расширением возможностей практической подготовки специалистов по защите информации.

Библиографический список

1. Модель многоканального управления учебным процессом высшей школы / А.Н. Данилов, Е.Л. Кон, Е.М. Кон, А.А. Южаков // Открытое образование. – 2012. – № 2. – С. 7–11.

2. 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. – Челябинск: Изд. центр Южно-Урал. гос. ун-та, 2012. – № 3–4(5–6). – С. 54–59.

3. Екимов О.Б. Методика разработки учебно-лабораторного комплекса для исследования систем защиты информации сложных военно-технических объектов: дис. … канд. техн. наук. – Пермь: Изд-во Перм. воен. ин-та ракет. войск, 2003. – 125 с.

4. Миронова А.А., Шабуров А.С. Модель разработки учебно-лабораторного комплекса для подготовки специалистов по защите ин-

формации // Вестник УрФО. Безопасность в информационной сфере. – Челябинск: Изд. центр ЮУрГУ, 2015. – № 3(17). – С. 28–32.

5. Капгер И.В., Журилова Е.Е., Миронова А.А. О разработке учебно-лабораторного стенда для изучения аппаратного модуля доверенной загрузки «Аккорд» // Вестник Пермского национального исследовательского политехнического университета. Электротехника, информационные технологии, системы управления – Пермь: Изд-во Перм. нац. исслед. политехн. ун-та, 2016. – № 17. – С. 131–142.

6. Шабуров А.С. О разработке учебно-лабораторного стенда для построения систем защиты информации на основе аппаратно-программного комплекса шифрования «Континент» // Научные исследования и инновации. – 2012. – Т. 6. – № 1–4. – С. 13–21.

7. Шабуров А.С., Борисов В.И. О применении сигнатурных методов анализа информации в SIEM-системах // Вестник УрФО. Безопасность в информационной среде. – Челябинск: Изд. центр ЮжноУрал. гос. ун-та, 2015. – № 17. – С. 23–27.

8. Шабуров А.С., Борисов В.И. Разработка модели защиты информации корпоративной сети на основе внедрения SIEM-системы // Вестник Пермского национального исследовательского политехнического университета. Электротехника, информационные технологии, системы управления – Пермь: Изд-во Перм. нац. исслед. политехн. ун-та, 2016. – № 19. – С. 111–124.

9. Шабуров А.С., Миронова А.А. Обнаружение компьютерных атак на основе функционального подхода // Вестник Пермского университета. Математика. Механика. Информатика. – 2015. – Вып. 4(31). – С. 110–115.

10. Данилов А.Н., Шабуров А.С. Концептуальный подход в решении задачи обеспечения безопасности информационно-управляющих систем // Вестник Казан. гос. техн. ун-та им. А.Н. Туполева. – 2012. – № 1. – С. 113–119.

11. Шабуров А.С. Разработка модели распознавания компьютерных атак на основе нейронной сети // Нейрокомпьютеры: разработка, применение. – 2016. – № 8. – С. 67–72.

12. Шабуров А.С., Рашевский Р.Б. Применение нейронных сетей для обеспечения безопасности информационно-управляющих систем критически важных объектов // Нейрокомпьютеры: разработка, применение. – 2014. – № 12. – С. 31–35.

13. Беззубцев О.А. Особенности сертификации средств защиты информации // Информационная безопасность. – 2012. – № 6 [Электронный ресурс]. – URL: http://www.securitycode.ru/products/continent/variants/ (дата обращения: 12.02.2017).

14. Аппаратно-программный комплекс шифрования «Континент» версия 3.5. Руководство администратора. Начало работы: метод. указ. / под ред. компании «Код Безопасности». – М.: Группа компаний «Информзащита», 2011. – 142 с.

15. Варианты применения АПКШ «Континент» 3.7 [Электронный ресурс]. – URL: http://www.securitycode.ru/products/continent/variants/ (дата обращения: 12.02.2017).

References

1. Danilov A.N., Kon E.L., Kon E.M., Iuzhakov A.A. Model' mnogokanal'nogo upravleniia uchebnym protsessom vysshei shkoly [Multichannel control model for higher school educational process]. *Otkrytoe obrazovanie*, 2012, no. 2, pp. 7-11.

2. Iuzhakov A.A., Shaburov A.S., Rashevskii R.B. O razrabotke uchebno-laboratornogo kompleksa dlia issledovaniia zashchishchennosti kriticheski vazhnykh ob"ektov [On the development of educational research laboratory complex for immunity critical facilities]. *Vestnik Ural'skogo federal'nogo okruga. Bezopasnost' v informatsionnoi sfere*. Chelyabinsk: Iuzhno-Ural'skii gosudarstvennyi universitet, 2012, no. 3-4(5-6), pp. 54-59.

3. Ekimov O.B. Metodika razrabotki uchebno-laboratornogo kompleksa dlia issledovaniia sistem zashchity informatsii slozhnykh voenno-tekhnicheskikh ob"ektov [Methods of development of teaching and laboratory facilities for the study of information security systems of complex military-technical objects.]. Ph.D. thesis. Permckii voennyi institut raketnykh voisk, 2003. 125 p.

4. Mironova A.A., Shaburov A.S. Model' razrabotki uchebno-laboratornogo kompleksa dlia podgotovki spetsialistov po zashchite informatsii [Model for development educational laboratory complex to train specialists in information protection]. *Vestnik Ural'skogo federal'nogo okruga. Bezopasnost' v informatsionnoi sfere*. Chelyabinsk: Iuzhno-Ural'skii gosudarstvennyi universitet, 2015, no. 3(17), pp. 28-32.

5. Kapger I.V., Zhurilova E.E., Mironova A.A. O razrabotke uchebno-laboratornogo stenda dlia izucheniia apparatnogo modulia doverennoi

zagruzki «Akkord» [About the developing of educational and laboratory bench for study of hardware module trusted boot «Accord»]. *Vestnik Permskogo natsional'nogo issledovatel'skogo politekhnicheskogo universiteta. Elektrotekhnika, informatsionnye tekhnologii, sistemy upravleniia*. Permckii natsional'nyi issledovatel'skii politekhnicheskii universitet, 2016, no. 17, pp. 131-142.

6. Shaburov A.S. O razrabotke uchebno-laboratornogo stenda dlia postroeniia sistem zashchity informatsii na osnove apparatno-programmnogo kompleksa shifrovaniia “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*, 2012, vol. 6, no. 1-4, pp. 13-21.

7. Shaburov A.S., Borisov V.I. O primenenii signaturnykh metodov analiza informatsii v SIEM-sistemakh [About the application of signatureanalysis method in the SIEM-systems]. *Vestnik Ural'skogo federal'nogo okruga. Bezopasnost' v informatsionnoi sfere*. Chelyabinsk: Iuzhno-Ural'skii gosudarstvennyi universitet, 2015, no. 17, pp. 23-27.

8. Shaburov A.S., Borisov V.I. Razrabotka modeli zashchity informatsii korporativnoi seti na osnove vnedreniia SIEM-sistemy [Developing model information protection corporate network based on the implementation of SIEM-system]. *Vestnik Permskogo natsional'nogo issledovatel'skogo politekhnicheskogo universiteta. Elektrotekhnika, informatsionnye tekhnologii, sistemy upravleniia*. Permckii natsional'nyi issledovatel'skii politekhnicheskii universitet, 2016, no. 19, pp. 111-124.

9. Shaburov A.S., Mironova A.A. Obnaruzhenie komp'iuternykh atak na osnove funktsional'nogo podkhoda [The detection of computer attacks based on the functional approach]. *Vestnik Permskogo universiteta. Matematika. Mekhanika. Informatika*, 2015, iss. 4(31), pp. 110-115.

10. Danilov A.N., Shaburov A.S. Kontseptual'nyi podkhod v reshenii zadachi obespecheniia bezopasnosti informatsionno-upravliaiushchikh sistem [Conceptual approach in solving the problem of information-control systems security]. *Vestnik Kazanskogo gosudarstvennogo tekhnicheskogo universiteta imeni A.N. Tupoleva*, 2012, no. 1, pp. 113-119.

11. Shaburov A.S. Razrabotka modeli raspoznavaniia komp'iuternykh atak na osnove neironnoi seti [Development of model for detection of computer attacks based on the neural network]. *Neirokomp'iutery: razrabotka, primenenie*, 2016, no. 8, pp. 67-72.

12. Shaburov A.S., Rashevskii R.B. Primenenie neironnykh setei dlia obespecheniia bezopasnosti informatsionno-upravliaiushchikh sistem kriticheski vazhnykh ob"ektov [Application of neural networks for security information and control systems of critical objects]. *Neirokomp'iutery: razrabotka, primenenie*, 2014, no. 12, pp. 31-35.

13. Bezzubtsev O.A. Osobennosti sertifikatsii sredstv zashchity informatsii [Features of certification of means of information protection]. *Informatsionnaia bezopasnost'*, 2012, no. 6, available at: http://www.securitycode.ru/products/continent/variants/ (accessed 12 February 2017).

14. Apparatno-programmnyi kompleks shifrovaniia «Kontinent» versiia 3.5. Rukovodstvo administratora. Nachalo raboty: metodicheskie ukazaniia [Hardware-software complex of encryption "Conti-nent" version 3.5. Administrator's guide. Beginning of work: methodical instructions.]. Moscow: Gruppa kompanii “Informzashchita”, 2011. 142 p.

15. Varianty primeneniia apparatno-programmnogo kompleksa shifrovaniia «Kontinent» 3.7 [Variants of application of the hardware-software complex "Continent" 3.7], available at: http://www.securitycode.ru/products/continent/variants/ (accessed 12 February 2017).

Сведения об авторах

Шабуров Андрей Сергеевич (Пермь, Россия) – кандидат технических наук, доцент кафедры автоматики и телемеханики Пермского национального исследовательского политехнического университета (614990, Пермь, Комсомольский пр., 29, e-mail: shans@at.pstu.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

Shaburov Andrey Sergeevich, (Perm, Russia) Ph.D. in Technical Sciences, Associate Professor of the Department of Automation and Telemechanics Perm National Research Polytechnic University (614990, Perm, 29, Komsomolsky pr., e-mail: shans@at.pstu.ru).

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

Получено 16.02.2017