Вестник науки и образования Северо-Запада России, 2018, Т.4, №1
ISSN 2413–9858

УДК 372.862

ПРИМЕНЕНИЕ ТЕХНОЛОГИИ И ПРОГРАММНОГО ОБЕСПЕЧЕНИЯ VIPNET В ПРОЦЕССЕ ПОДГОТОВКИ СПЕЦИАЛИСТОВ ПО ИНФОРМАЦИОННОЙ БЕЗОПАСНОСТИ

Д.Я. Околот, П.А. Корнев, И.Д. Рудинский

APPLICATION OF TECHNOLOGY AND SOFTWARE OF VIPNET IN THE PROCESS OF PREPARATION OF SPECIALISTS ON INFORMATION SECURITY

D.Y. Okolot, P.A. Kornev, I.D. Rudinskiy

Аннотация. В работе рассмотрены основные направления совершенствования системы подготовки квалифицированных специалистов по информационной безопасности на примере сотрудничества Балтийского информационного техникума и компании INFOTECS. Представлено описание одного из комплексов лабораторных работ, выполнение которого направлено на формирование практических навыков обеспечения информационной безопасности автоматизированных систем.

***Ключевые слова**: профессиональная подготовка; информационная безопасность; защита информации; подготовка специалистов.*

Abstract. In work mainstreams in perfecting of the system of training of qualified specialists in information security are considered in the work by the example of cooperation of the Baltic Information Technical School and the company INFOTECS. A description of one of the complexes of laboratory works is presented, the implementation of which is aimed at the formation of practical skills in ensuring the information security of automated systems.

***Key words:** professional training; information security; protection of the information; training of specialists.*

Информатизация и автоматизация играют важную роль в деятельности современных предприятий. Для того чтобы процессы автоматизированной обработки информации осуществлялись бесперебойно и безопасно, необходимо обеспечивать должную защиту и безопасность информационных потоков, циркулирующих в системе управления предприятием.

Особая актуальность массовой подготовки специалистов в области информационной безопасности (ИБ) дополнительно усиливается тем, что в современных условиях сведения о способах несанкционированного доступа к информации доступны практически любому желающему, причем количество попыток такого доступа непрерывно возрастает. В то же время, эффективную защиту информационных ресурсов может обеспечить только специалист в области ИБ, обладающий соответствующими профессиональными компетенциями [1].

В статье обосновывается целесообразность внедрения в процесс обучения будущих специалистов в области информационной безопасности технологий и программного обеспечения, разработанного компанией INFOTECS. Работа выполняется в Цикловой методической комиссии № 3 Автономной некоммерческой организации «Балтийский информационный техникум» по направлению подготовки «Обеспечение информационной безопасности автоматизированных систем».

В соответствии с требованиями федерального государственного образовательного стандарта 10.02.05 «Обеспечение информационной безопасности автоматизированных систем», выпускники технического колледжа должны не только владеть профессиональными

умениями и навыками, но и быть готовыми к освоению новых знаний, обеспечивающих их дальнейшую профессиональную пригодность, мобильность и конкурентоспособность [2].

В настоящее время многие руководители и специалисты крупных государственных и частных предприятий настоятельно рекомендуют учебным заведениям использовать в образовательном процессе программные продукты и технические средства, предназначенные для решения практических задач защиты информации и обеспечения информационной безопасности. Современный кадровый рынок ощущает потребность в высококвалифицированных специалистах по информационной безопасности, обладающих профильными знаниями и навыками работы с современным программным обеспечением, осуществляющим защиту информации [3].

Один из современных способов осуществления защищенного от посторонних обмена информацией с использованием сети Интернет между участниками информационных процессов заключается в организации виртуальных частных сетей (англ. Virtual Private Network – VPN), контролирующих и защищающих информационную систему предприятия от атак извне. Федеральный закон № 276 "О внесении изменений в закон "Об информации, информационных технологиях и о защите информации" ввел запрет на использование VPN-сервисов для посещения Интернет-ресурсов, доступ к которым ограничен по решению суда либо компетентными органами [4], однако их применение для защиты конфиденциальной информации в организациях и на предприятиях является легальным и оправданным.

Одним из ведущих отечественных разработчиков программно-аппаратных VPN-решений и средств криптографической защиты информации (СКЗИ), сертифицированных компетентными органами для применения на территории Российской Федерации, является компания INFOTECS (ИНФОрмационные ТЕхнологии и Коммуникационные Системы) [5]. Основная разработка компании – технология ViPNet – гибкое VPN-решение для безопасной передачи данных в защищенной сети. Продукты INFOTECS предназначены для решения широкого спектра задач организации защищенных виртуальных частных сетей и инфраструктуры открытых ключей (PKI).

Компания INFOTECS реализует специальную программу для образовательных учреждений высшего, среднего и дополнительного профессионального образования России и стран СНГ по обучению технологии ViPNet, что позволяет развивать учебно-методическую и материально-техническую базу образовательного учреждения и является предпосылкой обеспечения высокого качества образовательных услуг и подготовки специалистов [6]. С учетом указанных факторов руководством Балтийского информационного техникума в 2009 г. было принято решение о создании в техникуме авторизованного учебного центра по обучению студентов и специалистов по ИБ применению технологии ViPNet. Цель создания центра – профессиональная подготовка студентов, а также обучение и повышение квалификации клиентов и специалистов служб компьютерной безопасности в области построения комплексных систем ИБ и применения программных и аппаратных средств защиты информации в автоматизированных системах.

В учебном центре проводится обучение по следующим курсам:

- Администрирование средств защиты информации (СЗИ) ViPNet (Windows);
- Администрирование СЗИ ViPNet (Win&Lin);
- Программно-аппаратные комплексы ViPNet;
- Пользователь СЗИ ViPNet.

Занятия проводят специалисты, квалификация которых подтверждена сертификатами компании INFOTECS. Они работают на договорной основе и под методическим руководством Цикловой методической комиссии №3 Балтийского информационного техникума.

Для создания материально-технической базы учебного центра был выделен специализированный компьютерный класс, что позволило интегрировать программные продукты, реализующие технологию ViPNet, в процесс преподавания дисциплин

ISSN 2413–9858

профессионального цикла по направлению подготовки студентов техникума «Обеспечение информационной безопасности автоматизированных систем» и в полной мере реализовать их образовательный потенциал. При выполнении лабораторных работ и на практических занятиях студенты получают навыки работы в программных продуктах ViPNet Client, ViPNet Координатор, ViPNet Firewall, функционирующих под управлением операционных систем семейств Windows и Linux.

Компьютерный класс учебного центра оснащен современными программно-аппаратными средствами, необходимыми для проведения лабораторных работ и практических занятий. Локальная сеть компьютерного класса подключена к Интернету и интегрирована в корпоративную сеть компании «INFOTECS», что позволяет на реальных примерах демонстрировать студентам и слушателям основные сервисы и возможности защищенных виртуальных частных сетей. В ходе подготовки специалистов в области информационной безопасности используются сертифицированные компетентными органами средства защиты информации.

В авторизованном учебном центре проводятся занятия со студентами техникума, получающими среднее профессиональное образование по специальности 10.02.05 «Обеспечение информационной безопасности автоматизированных систем». В рабочую программу дисциплины «Программно-аппаратные средства защиты информации» введены следующие разделы, связанные с изучением технологии ViPNet и продуктов INFOTECS:

- технология построения сетей VPN ViPNet;
- система защиты информации ViPNet;
- администрирование системы защиты информации ViPNet;
- удостоверяющий центр ViPNet;
- программный комплекс ViPNet Client;
- комплексная защита конфиденциальной информации;
- практикум по применению программного обеспечения (ПО) ViPNet.

В качестве примера разработанных учебно-методических материалов рассмотрим состав и содержание лабораторного практикума «Администрирование системы защиты информации ViPNet», основанного на учебно-методическом пособии [7] (таблица 1).

Таблица 1 – Состав и содержание лабораторного практикума «Администрирование системы защиты информации ViPNet»

Название работы	**Описание**
Лабораторная работа 1. Развертывание защищенной сети ViPNet	Задание 1.1. Установка ПК ViPNet Administrator 4 Задание 1.2. Создание структуры защищенной сети Задание 1.3. Настройка резервного копирования данных и восстановление данных в ПО ViPNet Administrator Задание 1.4. Развертывание рабочего места помощника главного администратора Задание 1.5. Дополнительное задание. Миграция ПО ViPNet Administrator Контрольные вопросы
Лабораторная работа 2. Модификация защищенной сети и настройка политик безопасности на узлах	Задание 2.1. Модификация защищенной сети Задание 2.2. Компрометация Задание 2.3. Настройка политик безопасности в ViPNet Policy Manager Задание 2.4. Дополнительное задание Контрольные вопросы
Лабораторная работа 3. Межсетевое	Задание 3.1. Установка ViPNet Coordinator в качестве межсетевого шлюза

ISSN 2413–9858

взаимодействие	Задание 3.2. Первоначальная настройка межсетевого взаимодействия Задание 3.3. Модификация межсетевого взаимодействия Задание 3.4. Дополнительное задание Контрольные вопросы
Лабораторная работа 4. Работа с ViPNet Coordinator 4 for Windows	Задание 4.1. Настройка локальных и транзитных фильтров открытой сети Задание 4.2. Настройка фильтров защищенной сети Задание 4.3. Настройка трансляции адресов (NAT) Задание 4.4. Туннелирование в ViPNet Coordinator Задание 4.5. Дополнительное задание Контрольные вопросы
Лабораторная работа 5. Защита АРМ пользователя на основе технологии ViPNet	Задание 5.1. ViPNet Client 4 – VPN и персональный сетевой экран Задание 5.2. Криптопровайдер ViPNet CSP Задание 5.3. Работа с приложениями ViPNet Задание 5.4. Дополнительное задание Контрольные вопросы

Проблематика практического применения технологии ViPNet и продуктов INFOTECS также рассматривается и в других дисциплинах учебного плана специальности «Обеспечение информационной безопасности автоматизированных систем».

Функционирование авторизованного учебного центра позволяет Балтийскому информационному техникуму не только готовить компетентных специалистов со средним профессиональным образованием в сфере информационной безопасности и защиты информации, но и оказывать дополнительные образовательные услуги по этому направлению, ориентированные на:

- повышение квалификации специалистов по информационной безопасности, как имеющих, так и не имеющих опыт работы с программными продуктами INFOTECS;
- профессиональную переподготовку желающих получить базовые знания и умения в области практического применения технологии ViPNet и продуктов INFOTECS;
- презентации новых продуктов INFOTECS и консультирование по их эффективному использованию.

Слушатели курсов имеют возможность получить документы установленного образца о повышении квалификации, а также получить именной сертификат установленного образца по каждому прослушанному курсу.

Многолетнее функционирование авторизованного учебного центра АНО БИТ убедительно свидетельствует о значительном потенциале учреждений среднего профессионального образования, осуществляющих подготовку по специальности 10.02.05 «Обеспечение информационной безопасности автоматизированных систем», в сфере переподготовки и повышения квалификации практикующих специалистов по информационной безопасности. Стратегическое партнерство с ведущим отечественным разработчиком средств обеспечения информационной безопасности – компанией «INFOTECS» – позволяет, в случае необходимости, оперативно обновлять либо дополнять спектр изучаемых средств и технологий, а также изменять объем учебных занятий в соответствии с логикой образовательного процесса и реальными потребностями обучающихся. В то же время, наличие у выпускников техникума знаний о современных технологиях и продуктах, разработанных компанией «INFOTECS», и обладание умениями применять на практике соответствующие программно-аппаратные средства защиты

информации и обеспечения информационной безопасности повысит их конкурентоспособность и востребованность на рынке труда.

ЛИТЕРАТУРА

1. Рудинский И.Д., Околот Д.Я. Проблемы и задачи подготовки специалистов по информационной безопасности в системе среднего специального образования // Известия Балтийской государственной академии рыбопромыслового флота. 2017. № 4 (42). С. 63-69. [Электронный ресурс]. Режим доступа: http://bgarf.ru/science/journal-izvestia/42-2017/nepreryvn-professional.pdf

2. Приказ Минобрнауки России № 1553 от 09.12.2016 «Об утверждении федерального государственного стандарта среднего профессионального образования по специальности 10.02.05 «Обеспечение информационной безопасности автоматизированных систем». [Электронный ресурс]. Режим доступа: http:// минобрнауки.рф/документы/9881/файл/9054/Приказ%20№%201553%20от%2009.12.2016.pdf (дата обращения 01.01.2018).

3. Лихачев В. Кадровое обеспечение информационной безопасности. // Кадровик. Кадровый менеджмент. 2007. №12 [Электронный ресурс]. Режим доступа: http://hr-portal.ru/article/kadrovoe-obespechenie-informacionnoy-bezopasnosti (дата обращения 01.01.2018).

4. Федеральный закон № 276 от 29.07.2017 «О внесении изменений в закон "Об информации, информационных технологиях и о защите информации». [Электронный ресурс]. Режим доступа: http://www.consultant.ru/document/cons_doc_LAW_221230// (дата обращения 01.01.2018).

5. ОАО «INFOTECS». Официальный сайт компании. [Электронный ресурс]. Режим доступа: http://infotecs.ru/ (дата обращения 01.01.2018).

6. Малюк А.А., Алексеева И.Ю. Культура информационной безопасности как элемент подготовки специалистов по защите информации // Вестник РГГУ. Серия: документоведение и архивоведение. информатика. защита информации и информационная безопасность. 2016. С. 45-53.

7. Чаплыгин В.Е., Чефранова А.О., Алабина Ю.Ф. Администрирование системы защиты информации ViPNet версии 4. Учебно-методическое пособие / Под ред. докт. пед. наук, профессора А.О. Чефрановой. Москва: ОАО «INFOTECS». 2017. 188 с.

REFERENCES

1. Rudinskiy I.D., Okolot D.Ya. *Problemy i zadachi podgotovki spetsialistov po informatsionnoy bezopasnosti v sisteme srednego spetsial'nogo obrazovaniya* [Problems and tasks of specialists' training on information security in the system of secondary education] *Izvestiya Baltiyskoy gosudarstvennoy akademii rybopromyslovogo flota.* 2017. № 4 (42), pp. 63-69. [Electronic resource]. Available at: http://bgarf.ru/science/journal-izvestia/42-2017/nepreryvn-professional.pdf

2. *Prikaz Minobrnauki Rossii № 1553 ot 09.12.2016 «Ob utverzhdenii federal'nogo gosudarstvennogo standarta srednego professional'nogo obrazovaniya po spetsial'nosti 10.02.05 «Obespechenie informatsionnoy bezopasnosti avtomatizirovannykh sistem»* [The Ministry of education of Russia № 1553 from 09.12.2016 "On approval of the Federal state standard of secondary professional education on a speciality 10.02.05 "information security of automated systems".] [Electronic resource]. Available at: http:// минобрнауки.рф/документы/9881/файл/9054/Приказ%20№%201553%20от%2009.12.2016.pdf (accessed 01.01.2018).

3. Likhachev V. *Kadrovoe obespechenie informatsionnoy bezopasnosti* [Staffing of information security]. *Kadrovik. Kadrovyy menedzhment.* 2007. № 12 [Electronic resource]. Available at: http://hr-portal.ru/article/kadrovoe-obespechenie-informacionnoy-bezopasnosti (accessed 01.01.2018).

4. *Federal'nyy zakon № 276 ot 29.07.2017 «O vnesenii izmeneniy v zakon "Ob informatsii, informatsionnykh tekhnologiyakh i o zashchite informatsii»* [Federal law No. 276 of 29.07.2017 «On amendments to the law "On information, information technologies and protection of information»]. [Electronic resource]. URL: http://www.consultant.ru/document/cons_doc_LAW_221230 (accessed 01.01.2018).

5. OAO «INFOTECS». Ofitsial'nyy sayt kompanii [The company's official website]. [Electronic resource]. Available at: http://infotecs.ru/ (accessed 01.01.2018).

6. Malyuk A.A., Alekseeva I.Yu. *Kul'tura informatsionnoy bezopasnosti kak element podgotovki spetsialistov po zashchite informatsii* [Culture information security as an element of training in information security] *Vestnik RGGU. Seriya: dokumentovedenie i arkhivovedenie. informatika. zashchita informatsii i informatsionnaya bezopasnost'*. 2016, pp. 45-53.

7. Chaplygin V.E., Chefranova A.O., Alabina Yu.F. *Administrirovanie sistemy zashchity informatsii ViPNet versii 4. Uchebno-metodicheskoe posobie* [System Administration information protection ViPNet version 4. Educational-methodical manual]. Edit. Prof. A.O. Chefranova. Moskva: OAO «INFOTECS» Publ. 2017. 188 p.

ИНФОРМАЦИЯ ОБ АВТОРАХ

Околот Денис Ярославович

Калининградский государственный технический университет, г. Калининград, Россия, аспирант кафедры систем управления и вычислительной техники, АНО «Балтийский информационный техникум», преподаватель.

E-mail: dokolot@kantiana.ru

Корнев Павел Александрович

Учебный центр «ИнфоТеКС», г. Москва, Россия, старший преподаватель, кандидат технических наук.

E-mail: pavel.kornev@infotecs.ru

Рудинский Игорь Давидович

Калининградский государственный технический университет, г. Калининград, Россия, доктор педагогических наук, профессор кафедры систем управления и вычислительной техники.

E-mail: idru@yandex.ru

Okolot Denis Yaroslavovich

Kaliningrad State Technical University, Kaliningrad, Russia, Postgraduate student of the Department of Control Systems and Computer Engineering, lecturer of the «Baltic information technical school», Kaliningrad, Russia.

E-mail: dokolot@kantiana.ru

Kornev Pavel Aleksandrovich

Educational Center «Infotecs», Moscow, Russia, senior lecturer, Candidate of Technical Sciences.

E-mail: pavel.kornev@infotecs.ru

Rudinskiy Igor' Davidovich

Kaliningrad State Technical University, Kaliningrad, Russia, Doctor of Pedagogical Sciences, Professor, Department of Control Systems and Computer Engineering.

E-mail: idru@yandex.ru

Корреспондентский почтовый адрес и телефон для контактов с авторами статьи:
236022, Калининград, Советский пр., 1, КГТУ, ГУК, каб. № 261/3, И.Д. Рудинский
8 (4012) 995942