DOI: 10.17117/na.2016.11.02.281

<http://ucom.ru/doc/na.2016.11.02.281.pdf>

Поступила (Received): 05.11.2016

Шафеев Д.Е., Когай Г.Д., Тен Т.Л. Подготовка специалистов по информационной безопасности в Казахстане

Shafeev D.E., Kogai G.D., Ten T.L.
Training of specialists in information security in Kazakhstan

Рассмотрены вопросы разработки дополнительной профессиональной программы профессиональной переподготовки «Специалист по безопасности». Исследовано текущее состояние информационной безопасности в Казахстане, основные проблемы и тенденции, обусловившие актуальность разработки программы и ее содержания. Представлены структура программы, разработанные учебно-методические материалы

Ключевые слова: информационная безопасность, профессиональная переподготовка, программа профессиональной переподготовки «Специалист по безопасности»

We consider the development of additional professional retraining programs "security Specialist". Investigated the current state of information security in Kazakhstan, the main problems and trends contributing to the importance of the program and its content. The structure of the program developed educational materials

Key words: information security, professional retraining, professional retraining program "security Specialist"

Шафеев Даниил Евгеньевич

Студент

Карагандинский государственный технический университет

г. Караганда, Бульвар Мира, 56

Shafeev Daniel Evgenievich

Student

Karaganda state technical university

Karaganda, Boulevard Mira, 56

Когай Галина Давыдовна

Кандидат технических наук, профессор, старший преподаватель

Карагандинский государственный технический университет

г. Караганда, Бульвар Мира, 56

Kogay Galina Davydovna

Candidate of Engineering Sciences, Professor, Senior Teacher

Karaganda state technical university

Karaganda, Boulevard Mira, 56

Тен Татьяна Леонидовна

Доктор технических наук, профессор, старший преподаватель

Карагандинский государственный технический университет

г. Караганда, Бульвар Мира, 56

Ten Tatyana Leonidovna

Doctor of Engineering Sciences, Professor, Senior Teacher

Karaganda state technical university

Karaganda, Boulevard Mira, 56

В настоящее время продолжается рост отрасли информационной безопасности, что объясняется как ростом угроз информационной безопасности, так и ужесточением законодательства в области защиты конфиденциальной

информации в Казахстане и растущей популярностью внедрения мировых стандартов по управлению рисками. Задача обеспечения информационной безопасности на предприятиях ложится на плечи специалиста по информационной безопасности. В связи с этим казахстанские университеты, объединившиеся для выполнения TEMPUS project «PICTET: EQF-based professional ICT training for Kazakhstan», определили обязательной разработку дополнительной профессиональной программы переподготовки «Специалист по безопасности» (Security Specialist) с присвоением квалификации (степени) «Специалист по безопасности» (Senior Security Specialist) и «Ведущий специалист по безопасности» (Lead Security Specialist).

Текущее состояние информационной безопасности в Казахстане

Хотя Казахстан не входит в зону наиболее активной киберпреступности, государство все же попадает в число стран второго уровня по активности преступности в интернет-пространстве вместе с Румынией, Украиной и Латвией, составляющих 22% от общей киберпреступной деятельности в мире [1].

Правительства Казахстана активно работает в рамках Шанхайской организации сотрудничества – региональной организации, задачей которой провозглашено укрепление безопасности с координацией сил и разработкой общего механизма информационной безопасности государств-участников. Так, в 2010 году парламентом Казахстана был принят Закон «О ратификации соглашения между государствами-членами Шанхайской организации сотрудничества о сотрудничестве в сфере международной информационной безопасности». Казахстаном был подписан Регламент международной электросвязи с поправками, поддерживающими усиленный контроль государства над национальными сегментами глобального интернета. Эти поправки были направлены на передачу Организации Объединенных Наций контроля над управлением глобальным интернетом и, в результате, на зонирование киберпространства.

Более 300 законодательных актов Казахстана прямо или косвенно контролируют среду инфо – и телекоммуникационного сектора.

Учебно-методические материалы, разработанные в ходе реализации проекта

При разработке учебно-методического сопровождения программы авторы учитывали, что процесс защиты информации заключается не только в разовой разработке организационных мероприятий по информационной безопасности и настройке средств защиты информации, а также сопровождается аудитом существующей системы безопасности, построением модели угроз и их анализом, составлением нормативно-технической документации и поддержкой технических средств ее защиты. Для этого было разработано учебное пособие «Управление информационной безопасностью» [14], ориентированное наработку практических навыков у слушателей программы, в том числе – с применением интерактивных средств обучения и виртуального моделирования объектов защиты. Учебное пособие было создано с использованием в изучении программно-аппаратных комплексов и базовых информационных технологий, популярных в Казахстане.

Учебное пособие «Управление информационной безопасностью» состоит из 12 тематических разделов, содержащих теоретическое описание и практические задания, каждое из которых включает выполнение нескольких лабораторных работ. В пособии описаны лабораторные работы открытого доступа, которые могут проводиться в Казахстане. Изложенный в пособии материал охватывает широкий круг вопросов обеспечения информационной безопасности.

Приведены теоретические и практические материалы по работе с системным сканером «Ревизор сети и системы», предназначенным для использования администраторами и службами информационной безопасности локальных вычислительных сетей и автоматизированных систем, а также органами по аттестации объектов информатизации в целях централизованного проведения инвентаризации программных и технических ресурсов, фиксации настроек, обнаружения уязвимостей, контроля защищенности и автоматизированной проверки соответствия заданным требованиям локальных узлов автоматизированных систем.

Описаны базовые способы настройки системы комплексного анализа защищенности «Сканер-ВС», необходимого для определения топологии и инвентаризация ресурсов сети, поиска уязвимостей, локального и сетевого аудита стойкости паролей, перехвата и анализа сетевого трафика, аудита программного обеспечения и аппаратной конфигурации, контроля целостности, аудита защищенности WI-FI сетей. Приведены задания по настройке базовых элементов системы безопасности операционных систем семейства Windows.

Рассмотрены особенности программно-аппаратного комплекса Страж NT, с помощью которых слушатели могут устанавливать и снимать системы защиты информации, выполнять первоначальную настройку их механизмов, решать проблемы при возникновении внештатных ситуаций, которые могут возникнуть при установке и снятии системы защиты информации. Рассмотрены вопросы использования аппаратных средств для идентификации и аутентификации пользователей с использованием плат аппаратной поддержки на примере системы SecretNet, в т.ч. настройка управления доступом к системным и аппаратным ресурсам, избирательное и полномочное разграничение доступа с использованием программно-аппаратного комплекса «Соболь». Описано использование системы защиты информации eToken, позволяющей производить аутентификацию в операционной системе при помощи физического объекта.

Рассмотрены способы обнаружения на компьютере вредоносных программ, основные методы по устранению последствий вирусных инцидентов с использованием и без использования антивирусного программного обеспечения. Рассмотрена работа приложения Kaspersky Endpoint Security 10 – средства антивирусной защиты, позволяющего осуществить проверку операционной системы и съемных устройств от вирусных программ.

Описаны основные особенности и базовые настройки оборудования Cisco для формирования основных понятий и знаний о настройках удаленного подключения к командной оболочке маршрутизатора, рассмотрения основных вопросов безопасности, связанных с данным подключением; получения навыков

настройки протоколов Telnet, SSH, NTP на маршрутизаторе, установки и настройки TFTP сервера.

Заключение

В 2018 г. заканчивается срок реализации нашего проекта, заканчивается формальная сторона отношений вузов, скрепленная контрактом Темпус, но останутся партнерские отношения, способствующие актуализации разработанных программ, сотрудничеству вузов, объединенные порталом P1CTET-TEMPUS.

Список используемых источников:

1. Служба реагирования на компьютерные инциденты. Киберпреступность – угрозы и прогнозы. URL: [hUp://kz-cert.kz/ru/presscenter/publication/?doc=23](http://kz-cert.kz/ru/presscenter/publication/?doc=23)
2. Российская газета – Спецвыпуск. №6076. (100). URL: <http://rg.ru/2013/05/14/uslugi.html>
3. Tadviser. Государство. Бизнес. ИТ. URL: <http://www.tadviser.ru/index.php/>
4. UN E-Government Survey 2014 // United Nations Public Administration Country Studies, 2014. URL: <https://publicadministration.un.org/egovkb/Reports/UN-E-Governnient-Survey-2014>
5. Проект приказа Министерства труда и социальной защиты РФ «Об утверждении профессионального стандарта специалиста по информационной безопасности». URL: <http://base.consultant.ru/cons/cgi/online.cgi?req=doc;base=PNPA;n=4143;dst=1000> 19
6. Базовая модель угроз безопасности персональных данных при их обработке в информационных системах персональных данных (выпуска). ФСТЭК России, 2008 год.

© 2016, Шафеев Д.Е., Когай Г.Д., Тен Т.Л.
Подготовка специалистов по информационной
безопасности в Казахстане

© 2016, Shafeev D.E., Kogai G.D., Ten T.L.
Training of specialists in information security in
Kazakhstan