УДК 004:37

А.Н. Хлебников*

ОБЕСПЕЧЕНИЕ ИНФОРМАЦИОННОЙ БЕЗОПАСНОСТИ СОВРЕМЕННОГО УЧЕБНОГО ЗАВЕДЕНИЯ

В статье рассматривается проблемы обеспечения информационной безопасности и существующие методики внедрения информационных технологий для обеспечения информационной безопасности для современного учебного заведения.

Ключевые слова: информационная безопасность учебного заведения, защита персональных данных, программно-технические решения обеспечения информационной безопасности.

С увеличением доступности Интернета и стремительного развития средств коммуникации так же увеличиваются потребности обучающихся в доступности сервисов вне защищенного периметра не в ущерб информационной безопасности учреждения. Эти вопросы рассматриваются в работах ряда авторов.

В статье бизнес-консультанта Cisco по информационной безопасности Алексея Лукацкого [4] рассмотрены основные задачи обеспечения информационной безопасности современного учебного заведения:

– организация защищенного доступа к учебным материалам и системам удаленного обучения,

– защита информации ограниченного доступа (персональные данные, коммерческая тайна и т.п.),

– защита интеллектуальной собственности,

– выполнение требований законодательства в области информационной безопасности (федеральный закон «О персональных данных» от 27.07.2006 г. № 152-ФЗ, федеральный закон «О защите детей от информации, причиняющей вред их здоровью и развитию» от 29.12.2010 г. № 436-ФЗ и т.д.).

Современное крупное учебное заведение и его корпоративная сеть – это многоуровневая иерархическая среда, в которой сталкиваются интересы и данные разных групп пользователей. В учебном заведении встречаются следующие категории пользователей: студенты университета и студенты, приехавшие в университет по обмену; профессорско-преподавательский состав, сотрудники и администрация; школьники, посещающие подготовительные курсы перед поступлением в учебное заведение; посетители платных курсов и курсов повышения квалификации, предлагаемых учебным заведением.

Поскольку периметр классической корпоративной информационной сети учебного заведения продолжает размываться, смартфоны, планшеты и иные оконечные устройства с веб-приложениями или специализированными АРМами необратимо меняют образовательный процесс, предоставляя возможность

* Хлебников Александр Николаевич – магистрант, кафедра информатики и кибернетики, Байкальский государственный университет, г. Иркутск, e-mail: khlebnikovan@bgu.ru.

получать доступ к учебным сервисам за пределами учебного заведения: из общежития, другого учебного заведения, куда обучающиеся отправляются для обмена опытом, и т.п. Вместе с тем при внедрении концепции доступа отовсюду возникает целый ряд задач информационной безопасности, которые необходимо решить. В таком случае нужно обеспечить:

– предотвращение несанкционированного доступа устройств в защищенный периметр учебного заведения,

– выполнение требований и рекомендаций существующих политик информационной безопасности,

– обеспечение возможности контроля подключенных к корпоративной сети устройств на предмет соответствия действующим политикам информационной безопасности,

– обеспечение организацией логического разделения корпоративной сети на зоны безопасности без изменения существующей инфраструктуры.

Образовательное учреждение – это огромный объем разнообразной конфиденциальной информации, требующей защиты. Речь идет о:

– персональных данных студентов, преподавателей, администрации и сотрудников учебного заведения,

– сведениях, составляющих коммерческую тайну учебного заведения обеспечивающих конкурентную способность в области предоставления более качественного образования,

– разработанных учебным заведением образовательных материалах, доступ к которым должен быть либо ограничен, либо контролируемым, т.к. они представляют собой интеллектуальную собственность.

Помимо защиты информации ограниченного доступа, необходимо обеспечивать безопасность информационных систем образовательного процесса. Случайный или целенаправленный вывод этих систем из строя может остановить процесс обучения и нарушить договорные условия (в случае платного обучения).

Кроме защиты информационных систем и информации, система обеспечения информационной безопасности должна давать возможность выполнять законодательные инициативы, направленные на защиту прав и интересов различных групп граждан и организаций. К нормативным актам, которые учебное заведение обязано выполнять, в первую очередь относятся:

– федеральный закон от 27 июля 2006 года № 152-ФЗ «О персональных данных»;

– федеральный закон от 28 июля 2012 года № 139-ФЗ «О внесении изменений в федеральный закон «О защите детей от информации, причиняющей вред их здоровью и развитию» и отдельные законодательные акты Российской Федерации по вопросу ограничения доступа к противоправной информации в сети Интернет»;

– федеральный закон от 2 июля 2013 года № 187-ФЗ «О внесении изменений в законодательные акты Российской Федерации по вопросам защиты интеллектуальных прав в информационно-телекоммуникационных сетях».

Комплексное решение от Microsoft в области обеспечения информационной безопасности учебного заведения

Microsoft Forefront – это комплексное решение, повышающее защищенность и управляемость информационной безопасности в сетевой инфраструктуре учебного заведения. Продукты Microsoft Forefront легко интегрируются друг с другом и существующей инфраструктурой организации. Кроме того, их можно дополнять решениями сторонних производителей, что позволяет создавать законченные решения, обеспечивающие многоуровневую защиту.

Многоуровневая защита состоит из широкого спектра программного обеспечения:

– Клиентская безопасность обеспечивается антивирусным программным обеспечением – Microsoft Forefront Endpoint Protection;

– Серверная безопасность обеспечивается комплексом программного обеспечения (Microsoft Forefront Security for Exchange Server, Microsoft Forefront Security for SharePoint, Microsoft Forefront Security for Microsoft Office, Communications Server, Microsoft Forefront Unified Access Gateway, Microsoft Forefront Threat Management Gateway), направленного для минимизации угроз направленного за пределами защищенного периметра.

Решения от других вендоров в области обеспечения информационной безопасности учебного заведения

Целью данных решений является обеспечение безопасного доступа к внутренним информационным ресурсам организации с удаленных рабочих мест. Основное внимание при этом уделяется защите каналов связи, например, IPsec или SSL, а также аутентификации пользователей. Для достяжений данной цели существуют решения:

– Программный комплекс Crypton IP Mobile предназначен для защиты данных, передаваемых по компьютерным сетям. Комплекс позволяет создавать поверх общедоступных сетей виртуальные частные сети (VPN) с «прозрачным» шифрованием информации (полным или выборочным) по алгоритму ГОСТ 28147-89 и контролем целостности. Crypton IP Mobile соответствует требованиям ФСБ России к СКЗИ по классу КС1, КС2, КС3 (в зависимости от исполнения) и может использоваться для криптографической защиты конфиденциальной информации [5].

– Экспортный вариант шлюза безопасности «С-Терра Шлюз». Предназначен в первую очередь для отечественных заказчиков, осуществляющих свою деятельность за пределами Российской Федерации. Эксплуатация CSP VPN Gate E допускается как на территории Российской Федерации, так и за её пределами, что отражено в Формуляре на изделие ПК «CSP VPN Gate E», согласованном регулятором на стадии сертификации изделия и удостоверяющим его основные характеристики и комплект поставки. Это упрощает получение установленным законодательством порядком лицензии ФСТЭК на экспорт, необходимой для вывоза за пределы России сертифицированного СКЗИ [2].

– Продукты линейки Box Lite ориентированы в основном на индивидуальное использование и решение отдельных задач по защите информации. Данные продукты характеризуются удобством и простотой использования, облегченной функциональностью. В состав линейки входят как продукты по защите небольших локальных сетей и персональных компьютеров от атак из внешних сетей (ViPNet Office Firewall, ViPNet Personal Firewall), так и продукты для защиты конфиденциальной информации (ViPNet Safe Disk, ViPNet DISCguise и др.) Продукты линейки Box Lite сочетают в себе удобство и простоту использования с надежностью современных технологий защиты информации и ориентированы в основном на решение задач индивидуального пользователя и малого бизнеса. Некоторые из продуктов линейки Box Lite являются бесплатными или условно бесплатными и доступны для свободного скачивания [5].

– Программно аппаратный комплекс VipNet Coordinator HW 100 включает криптошлюз и межсетевой экран и позволяет безопасно подключить любое сетевое оборудование в виртуальную частную сеть, построенную с использованием продуктов VipNet. VipNet Coordinator HW 100 построен на базе ПО VipNet Coordinator Linux и выполняет в VipNet-сети функции ПО VipNet Coordinator, включая функцию VPN-сервера для доступа удаленных VPN-Клиентов, оснащенных ПО VipNet Client. Шифрование и защита от подмены пакетов осуществляются по ГОСТ 28147-89 [5].

Аппаратные решения в области обеспечения информационной безопасности учебного заведения

Существует множество аппаратных решений для обеспечения информационной безопасности:

– FORTIGATE – это многофункциональные сетевые устройства FortiGate обеспечивают экономически эффективную комплексную защиту на уровне сети, приложений и данных, в том числе от современных комбинированных многоуровневых атак без ущерба для производительности и доступности сети [3];

– FortiDB – это наиболее полное решение обеспечивающее безопасность баз данных и приложений, таких как: ERP, CRM, SCM и приложений собственной разработки [3];

– FortiWeb – это семейство межсетевых экранов для WEB и XML-приложений, которое обеспечивает защиту, балансировку и ускорение работы web-приложений, баз данных и обмена информацией между ними [3];

– PINEAPP MAIL-SECURE 1000 – это аппаратное решение обеспечивает защиту корпоративных серверов электронной почты, как от нацеленных, так и от не нацеленных угроз [2];

– FireEye Network Security Essentials – это решение, позволяющее минимизировать угрозы, которые могут привести к значительным финансовым потерям, благодаря высокоточному обнаружению и предотвращению современных кибератак [1].

Обеспечение информационной безопасности современного учебного заведения является обязательной процедурой, обеспечивающей повышение конкурентноспособности учебного заведения.

Список использованной литературы

1. FireEye Network Security Essentials [Электронный ресурс] // URL: https://www.fireeye.com/products/nx-network-security-products.html.

2. PINEAPP MAIL-SECURE 1000 [Электронный ресурс] // URL: http://www.pointlane.ru/solutions/antispam/pineapp-mailsecure-1000.

3. Линейка продуктов фирмы FORTINET [Электронный ресурс] // URL: https://www.fortinet.com/products/firewalls/firewall.html.

4. Обеспечение информационной безопасности современного ВУЗа инфраструктуры предприятия [Электронный ресурс] // URL: http://www.cisco.com/c/ru_ru/about/press/press-releases/2013/12-120613d.html.

5. Решения для безопасного удаленного доступа [Электронный ресурс] // URL: https://www.catalog.ib-bank.ru/katalog/147.