ПРИНЦИПЫ ОБЕСПЕЧЕНИЯ БЕЗОПАСНОСТИ ОБРАЗОВАТЕЛЬНЫХ ИНФОРМАЦИОННЫХ СЕТЕЙ

Ю.И. Воротницкий, Се Цзиньбао

Белорусский государственный университет, кафедра кибернетики,
просп. Независимости, 4, г. Минск, Республика Беларусь
телефон: + 375 17 2095217, факс: + 375 17 2265557; e-mail: vorotn@bsu.by
web: www.bsu.by

В докладе предлагаются подходы к обеспечению безопасности образовательных информационных сетей с учетом особенностей пользовательской аудитории, информационных ресурсов, типовых архитектурных решений. Подробно рассматриваются особенности постановки задач обеспечения безопасности образовательных сетей, типовая архитектура безопасности корпоративной образовательной сети, методики и средства управления доступом к внешним информационным ресурсам.

Ключевые слова – безопасность, информационные сети, образование

1 ПОСТАНОВКА ЗАДАЧИ ОБЕСПЕЧЕНИЯ БЕЗОПАСНОСТИ ОБРАЗОВАТЕЛЬНЫХ СЕТЕЙ

Сегодня, в условиях экспоненциального роста информации, процесс обучения немыслим без использования современных информационных технологий. Информатизация образования является основой педагогических инноваций, а современная информационная инфраструктура – средой для накопления и получения знаний [1]. Основу современной образовательной ИКИ составляют локальные и корпоративные сети учреждений образования, которые объединяются в национальные и международные образовательные сети.

Любая корпоративная образовательная сеть представляет собой целостную архитектуру, состоящую из четырех основных компонент.

1. Коммуникационная инфраструктура – каналы передачи, коммуникационное оборудование, серверы, рабочие станции, периферийное оборудование.
2. Сетевые технологии – совокупность протоколов, методов и средств, обеспечивающих сбор, хранение, обработку, передачу информации и доступ к ней. Это - технологии аутентификации и авторизации, DNS, Proxy, Web, системы управления базами данных, видеоконференции, потоковое видео, обеспечение качества обслуживания и др.
3. Информационные ресурсы – совокупность данных, организованных для получения информации. К таким ресурсам можно отнести сайты учебных заведений, массивы электронных документов, включая курсы лекций, методические и информационные материалы, электронные каталоги библиотеки, и т.д.
4. Организационно-правовая структура – правовые документы, регламентирующие интеллектуальную собственность; законодательные акты, регламентирующие работу пользователей в сети; правила работы в сети; политики безопасности, политики управления информационной средой и т.д.

Методы, технологии и средства обеспечения безопасности образовательных сетей должны разрабатываться, исходя из решаемых с помощью этих сетей задач, к которым, прежде всего, относятся:

- интеграция образовательных и научных ресурсов, базирующихся на различных стандартах и платформах;
- обмен научно-образовательной информацией в различных областях знаний (порталы, электронная почта, P2P, интернет-пейджеры и др.);
- организация дистанционного обучения (размещение учебных планов, электронных учебников, материалов семинаров и лабораторных работ, проведение консультаций в режиме on-line, осуществление контроля знаний);
- создание систем поиска образовательной и научной информации;
- предоставление мультисервисных услуг, в частности, трансляции видео конференций и лекций через глобальные и корпоративные сети;
- обеспечение работы в режиме виртуальных научных и учебных лабораторий;
- обеспечение работы в международных системах распределенной обработки и хранения информации в разных областях науки и образования;
- управление учебным процессом;
- управление образовательными учреждениями (сбор данных об учащихся и сотрудниках, взаимосвязь с родителями, электронные приемные).

Исходя из анализа этих задач и основываясь на опыте проектирования образовательных сетей [2,3] можно выделить следующие отличительные черты таких сетей, которые существенно влияют на постановки и методики решения задач обеспечения их безопасности.

1. Наличие наряду с традиционным внешним периметром сети, отделяющим защищенную сеть от внешнего мира, своеобразного «внутреннего периметра», отделяющего защищаемые внутренние ресурсы от массовых

пользователей, в первую очередь, учащихся. Действительно, на базе единой корпоративной сети не только обеспечивается доступ к внутренним и внешним образовательным ресурсам, но решаются задачи управления учебными заведениями, управления учебным процессом и другие, требующие обеспечения защиты соответствующих баз данных и разграничения доступа к ним. За пределами «внутреннего периметра» должны находиться локальные сети учебных классов, учебных лабораторий, общежитий, сети беспроводного доступа и т.п.

2. Высокая степень угроз безопасности со стороны «инсайдеров». Здесь речь идет не только о злоумышленных действиях обучаемых и сетевых атаках из-за пределов «внутреннего периметра». Серьезной также является проблема широкомасштабного внесения в сеть вредоносных программ массовыми пользователями, использующими самые разнородные ресурсы Интернет, электронную почту, обменивающимися информацией на сменных носителях.

3. Наличие необходимости доступа к разнообразным внешним информационным ресурсам. В корпоративной сети организации обычно можно ограничить категории пользователей, имеющих доступ к внешним ресурсам Интернет, но и четко указать, к каким типам ресурсов доступ нецелесообразен. В образовательных сетях понятие нежелательных ресурсов является более сложным (например, студенты-психологи могут изучать развлекательные сайты, а будущие менеджеры туризма – сайты, посвященные туризму, отдыху и путешествиям).

Разумеется, обеспечение безопасности образовательных сетей предполагает противодействие традиционным угрозам нарушения конфиденциальности информации, целостности информации и работоспособности сети (доступности информации). Вместе с тем, специфика образовательных сетей позволяет, на наш взгляд, отдельно рассматривать угрозу доступа к нежелательным информационным ресурсам. Действительно, вред от неприемлемой (порнография, терроризм, политический экстремизм и т.п.) и недостоверной (ошибочная, субъективная информация, воспринимаемая обучаемым как истинная) информации для широкой молодежной аудитории в образовательных сетях весьма значителен. С другой стороны, массовый доступ к не имеющим отношения к образовательной деятельности ресурсам (торренты, социальные сети и т.п.) поглощает значительную часть внешних каналов. (Например, трафик на социальную сеть «в контакте» из сети Белорусского государственного университета до ее блокирования занимал до 20% всего трафика университета). Большое число пользователей образовательных сетей, рост объемов мультимедийной информации в Интернет делает проблему ограничения доступа к внешним ресурсам еще более актуальной.

В связи с вышеизложенным, можно выделить наиболее актуальные направления разработок по обеспечению безопасности корпоративных образовательных сетей:

- разработка архитектурных решений, обеспечивающих структуризацию и сегментацию образовательной сети;
- использование эффективных решений для аутентификации для проверки подлинности пользователей и объектов сети, а также авторизации доступа к внутренним и внешним информационным ресурсам;
- разработка технологий обнаружения вторжений для активного исследования защищенности информационных ресурсов;
- создание централизованно управляемой системы антивирусной защиты;
- разработка методов и средств ограничения доступа к нежелательным внешним информационным ресурсам;
- разработка и внедрение политик безопасности, ориентированных на различные категории пользователей образовательной сети.

2 АРХИТЕКТУРА БЕЗОПАСНОСТИ КОРПОРАТИВНОЙ ОБРАЗОВАТЕЛЬНОЙ СЕТИ

Традиционная архитектура безопасности корпоративной сети состоит из периметра, обеспечивающего связь с внешними сетями (включает в себя пограничный маршрутизатор, межсетевой экран и сервера демилитаризованной зоны), и внутренней сети.

Для образовательной сети эта архитектура должна быть дополнена еще двумя зонами: зоной повышенного риска, в которую входят локальные сети учебных классов и лабораторий, общежитий и т.п., а также защищенной зоной (административные службы).

Защита периметра корпоративной сети - первичная задача обеспечения информационной безопасности. Внутри периметра функционируют наиболее критичные системы – приложения, базы данных, активное сетевое оборудование и другие. Поэтому решения в области безопасности периметра корпоративных образовательных сетей строятся таким образом, чтобы извне сеть была абсолютно непрозрачной, иметь регламентированные интерфейсы и протоколы, предотвращать несанкционированный доступ к внутренним ресурсам корпоративной сети, обеспечивать защиту от атак отказа в обслуживании узлов с внешними адресами, вирусных атак и защиту от спама.

Управление доступом в модуле корпоративного периметра осуществляется маршрутизатором и выделенным межсетевым экраном. Защита внешних серверов обеспечивается технологией демилитаризованной зоны, которая подключается на выделенный межсетевой экран. Удаленные пользователи, работающие через телефонные сети общего доступа, соединяются с корпоративной сетью по технологии виртуальных частных сетей (VPN). Дизайн модуля корпоративного периметра представлен на рисунке 1.

Внутренняя сеть учреждения образования – это наиболее защищенная часть корпоративной сети. Межсетевой экран обеспечивает ее безопасность со стороны внешней сети и демилитаризованной зоны. В корпоративных образовательных сетях обычно принимается базовый уровень информационной безопасности. При этом во внутренней сети может быть разрешен практически любой трафик.

Тем не менее, внутренняя корпоративная образовательная сеть разделена на несколько сегментов безопасности. Прежде всего, выделяется локальная сеть административных служб – защищенная зона. Это необходимо для того, чтобы отделить критические данные от общей корпоративной сети. На границе защищенной зоны установлен маршрутизатор, который дополнительно выполняет функции межсетевого экрана по управлению доступом посредством пакетной фильтрации.

Рис.1. Дизайн модуля периметра

Сети общежитий и сети учебных классов (зона повышенного риска) отделяются от общей университетской сети на канальном уровне модели OSI по технологии локальных виртуальных частных сетей (VLAN). В каждой сети общежитий и классов устанавливаются средства контроля трафика.

На канальном уровне по VLAN выделены подсети маршрутизаторов, сеть управления, сети отдельных подразделений. Предлагаемая архитектура внутренней сети, включающая в себя зону внутренней сети, зону повышенного риска, защищенную зону и сеть централизованного управления показана на рис. 2.

Во внутренней сети располагаются средства мониторинга безопасности сети – это сканеры уязвимостей, анализаторы протоколов. Регулярное тестирование сети позволяет обеспечить дополнительный уровень безопасности сети.

Архитектура безопасности корпоративных образовательных сетей всегда должна базироваться на концепции и политиках обеспечения сетевой безопасности корпоративной сети.

Модульное разделение корпоративной сети позволяет осуществлять поэтапное внедрение политик безопасности, начиная от критичных областей.

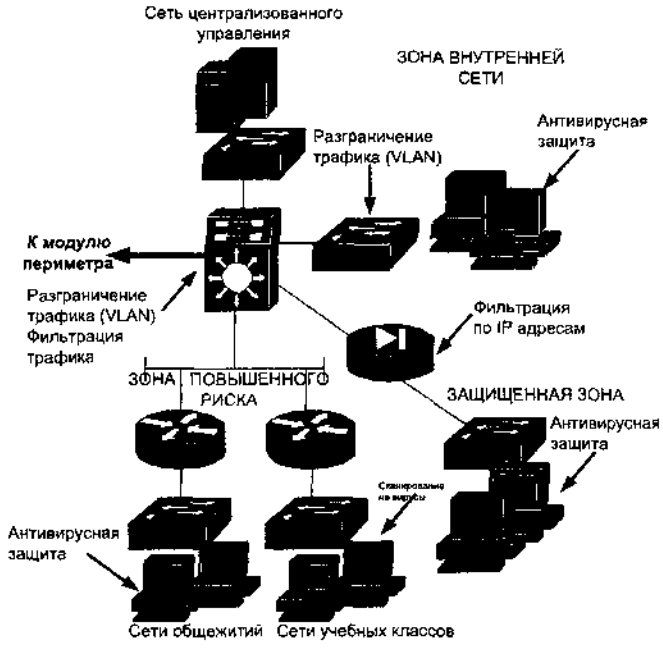

Рис.2. Дизайн модуля внутренней сети

3 УПРАВЛЕНИЕ ДОСТУПОМ К ВНЕШНЕМУ КОНТЕНТУ

Как отмечалось выше, задача управления доступом к внешним информационным ресурсам из образовательных сетей является весьма актуальной. Решить ее традиционными способами, такими как использование специального программного обеспечения, обращающегося к базам данных, классифицирующим Интернет-сайты и ограничивающего доступ к нежелательным сайтам, затруднительно.

Действительно, реализация известных механизмов онлайновой фильтрации не позволяет адекватно идентифицировать ресурсы, не имеющие отношения к научной и образовательной деятельности, массовый доступ к которым отвлекает учащихся, а порой и вызывает затруднения в доступе к сетевым ресурсам в силу перегрузки внешних каналов корпоративных сетей (ИР социальных сетей, таких как «В контакте», «Одноклассники» и т.п.). Значительная часть информации фильтруется «на входе» в сеть, что не эффективно в условиях внешнего канала с ограниченной пропускной способностью. Кроме того, соответствующие контент-фильтры достаточно дороги

На наш взгляд, необходимо ставить задачу не столько ограничения доступа к внешнему контенту, сколько управления этим доступом. Для этого целесообразно использовать специальные средства управления трафиком и специально разработанную для использования в образовательных сетях биллинговую систему [4].

Кроме того, целесообразно реализовать следующие мероприятия:

- насыщение корпоративной сети собственными сетевыми образовательным ресурсами и внедрение

единой сетевой системы управления этими ресурсами;
- целенаправленный отбор внешних образовательных ресурсов и их продвижение путем размещения ссылок на них на Интранет- и Интернет-сайтах учебных подразделений;
- использование специализированной поисковой системы, обрабатывающей рекомендуемые информационные источники.

Управление доступом к внешним информационным ресурсам может строиться с использованием механизмов, традиционно применяемых для авторизации доступа к ресурсам внутренним, таким как:
- разграничение прав пользователей;
- авторизация по ролям;
- использование списков контроля доступа;
- авторизация в соответствии с заданными правилами.

Авторами предлагается методика и программный комплекс, позволяющие обеспечить управление доступом путем анализа только востребованных пользователями сети внешних информационных ресурсов.

Предполагается, что все внешние ресурсы, к которым обращались пользователи сети помещаются в один из трех списков: «белый», «серый» или «черный». При первом обращении к ресурсу он помещается в «серый» список. В списке фиксируется url и число запросов к ресурсу. Также может сохраняться копия содержимого, к к которому обратился пользователь.

Запрос к ресурсу из «серого» или «белого» списка пропускается прокси-сервером, и пользователь получает доступ к этому ресурсу.

После накопления порогового числа запросов к ресурсу из «серого» списка (обычно от 1 до 100), специализированная поисковая система в период минимальной загрузки внешнего канала (ночью) осуществляет сканирование соответствующего url (причем не одной страницы, а сайта целиком).

Результаты сканирования поступают в модуль анализа контента, и в случае высокой вероятности его нежелательности, информация поступает администратору безопасности, принимающему окончательное решение о помещении проанализированного ресурса в «белый» или «черный» список.

Возможно ведение отдельных списков для различных категорий пользователей.

Использование поисковой машины для сбора контента по указанному адресу позволяет анализировать не только запрашиваемый ресурс (например, веб-страницу), но весь сайт, к которому относится запрос. Это (особенно с учетом задач образовательной сети) делает дальнейший анализ более адекватным.

Схема функционирования программного комплекса представлена на рис. 3.

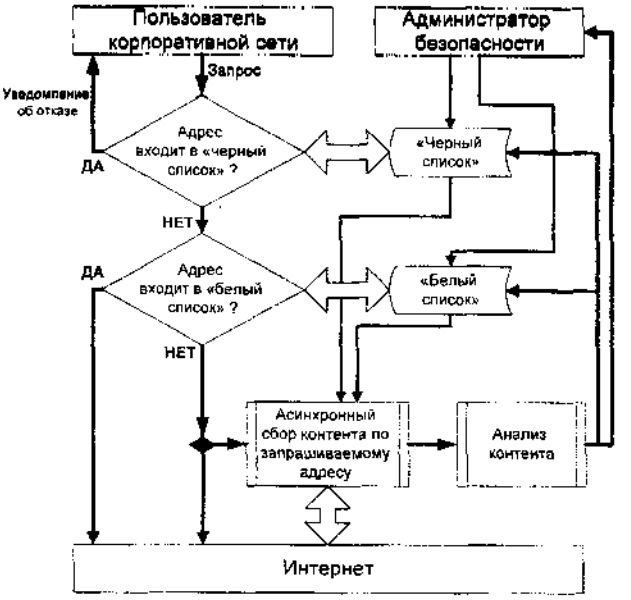

Рис. 3. Схема программного комплекса ограничения доступа к нежелательному контенту

4 ЗАКЛЮЧЕНИЕ

Предлагаемые в настоящем докладе принципы обеспечения безопасности образовательных информационных сетей основаны как на анализе доступных информационных источников, так и на опыте авторов. Часть предлагаемых решений апробирована в Белорусском государственном университете и Харбинском техническом университете (КНР).

ЛИТЕРАТУРА

[1] О некоторых вопросах стратегии информатизации образования Республики Беларусь / Ю.И. Воротницкий [и др.] // Информатизация образования. – 2003. - № 1. – С. 23-28.

[2] Концепция построения и развития отраслевой информационной среды системы образования республики Беларусь / Ю.И. Воротницкий [и др.] // ГИАЦ Минобразования Республики Беларусь, 2007. – 131с.

[3] Воротницкий Ю. И., Утко Л.З. Организация доступа к информационным ресурсам в корпоративной сети Белорусского государственного университета / Ю.И. Воротницкий, Л.З. Утко // Материалы научно-практической конференции «Управление информационными ресурсами». Минск, Редакционно-издательский центр Академии управления при Президенте Республики Беларусь, 2003. – С. 33-34. – 1 с.

[4] Воротницкий Ю.И. Технологии интеграции научно-информационной компьютерной сети Республики Беларусь во внешние сети / Ю.И. Воротницкий, А.В. Иода // Управление защитой информации. – 2004. Т. 8. № 2.– С. 170-171 – 2 с.