ПРОБЛЕМЫ ЗАЩИТЫ ОБРАЗОВАТЕЛЬНЫХ СЕТЕЙ ВУЗОВ

А.К. Хасанов
Алтайский государственный университет, г. Барнаул

Современные технологии обеспечения информационной безопасности (ИБ) помогают учебным заведениям решать стоящие задачи в следующих основных направлениях:
- организация защищенного доступа к образовательным материалам и системам;
- защита информации ограниченного доступа (персональные данные, коммерческая тайна и т.п.) и защита интеллектуальной собственности;
- выполнение требований законодательства в области информационной безопасности (защита персональных данных, защита прав на интеллектуальную собственность, защита детей от негативной информации). В современном вузе хранится и обрабатывается огромное количество различных данных, связанных не только с обеспечением учебного процесса, но и с научно-исследовательскими и проектно-конструкторскими разработками, персональные данные студентов и сотрудников, служебная, коммерческая и иная конфиденциальная информация. Рост преступлений в сфере высоких технологий диктует свои требования к защите ресурсов вычислительных сетей учебных заведений и ставит задачу построения собственной интегрированной системы безопасности. Ее решение предполагает наличие нормативно-правовой базы, формирование концепции безопасности, разработку мероприятий, планов и процедур по безопасной работе, проектирование, реализацию и сопровождение технических средств защиты информации (СЗИ) в рамках образовательного учреждения. Эти составляющие определяют единую политику обеспечения безопасности информации в вузе.

Специфика защиты информации в образовательной системе заключается в том, что вуз – публичное заведение с непостоянной аудиторией, а также место повышенной активности «начинающих киберпреступников». Основную группу потенциальных нарушителей в вузе составляют студенты, ряд из них имеют достаточно высокий уровень подготовки. Возраст (от 18 до 23 лет) и юношеский максимализм побуждают таких людей блеснуть знаниями перед сокурсниками: устроить вирусную эпидемию, получить административный доступ и «наказать» преподавателя, заблокировать выход в Интернет и т. д. Достаточно вспомнить, что

первые компьютерные правонарушения родились именно в вузе (червь Морриса) [4].

Особенности вуза как объекта информатизации связаны также с многопрофильным характером деятельности, обилием форм и методов учебной работы, пространственной распределенностью инфраструктуры (филиалы, представительства). Сюда же можно отнести и многообразие источников финансирования, наличие развитой структуры вспомогательных подразделений и служб (строительная, производственная, хозяйственная деятельность), необходимость адаптации к меняющемуся рынку образовательных услуг, потребность в анализе рынка труда, отсутствие общепринятой формализации деловых процессов, необходимость электронного взаимодействия с вышестоящими организациями, частое изменение статуса сотрудников и обучаемых. Несколько облегчает проблему то, что вуз представляет собой стабильную, иерархическую по функциям управления систему, обладающую всеми необходимыми условиями жизнедеятельности и действующую на принципах централизованного управления (последнее означает, что в управлении задачами информатизации может активно использоваться административный ресурс).

Указанные выше особенности обусловливают необходимость соблюдения следующих требований:

- комплексная проработка задач информационной безопасности, начиная с концепции и заканчивая сопровождением программно-технических решений;
- привлечение большого числа специалистов, владеющих содержательной частью деловых процессов;
- использование модульной структуры корпоративных приложений, когда каждый модуль покрывает взаимосвязанную группу деловых процедур или информационных сервисов при обеспечении единых требований к безопасности;
- применение обоснованной последовательности этапов в решении задач информационной безопасности;
- документирование разработок на базе разумного применения стандартов, что гарантирует создание успешной системы;
- использование надежных и масштабируемых аппаратно-программных платформ и технологий различного назначения, обеспечивающих необходимый уровень безопасности.

С точки зрения архитектуры в корпоративной информационной среде можно выделить три уровня, для

обеспечения безопасного функционирования которых необходимо применять различные подходы:
- оборудование вычислительной сети, каналов и линий передачи данных, рабочих мест пользователей, системы хранения данных;
- операционные системы, сетевые службы и сервисы по управлению доступом к ресурсам, программное обеспечение среднего слоя;
- прикладное программное обеспечение, информационные сервисы и среды, ориентированные на пользователей.

При создании комплексной информационной сети необходимо обеспечить межуровневое согласование требований по безопасности к выбираемым решениям или технологиям. Так, на втором уровне архитектура комплексной информационной сети многих вузов представляет собой разрозненные и слабо связанные подсистемы с разными операционными средами, согласованные друг с другом только на уровне закрепления IP-адресов или обмена сообщениями. Причинами плохой системной организации комплексной информационной сети является отсутствие утвержденной архитектуры комплексной информационной сети, наличие нескольких центров ответственности за развитие технологий, которые действуют несогласованно. Проблемы начинаются с нежелания управлять выбором операционных сред в подразделениях, когда ключевые технологические решения полностью децентрализованы, что резко снижает уровень безопасности системы.

Вузы, имеющие четкую стратегию развития информационных технологий, единые требования к информационной инфраструктуре, политику информационной безопасности и утвержденные регламенты на основные компоненты комплексной информационной сети, отличаются, как правило, сильным административным ядром в управлении и высоким авторитетом руководителя ИТ-службы [5]. В таких вузах могут использоваться различные операционные среды или системы среднего слоя, но это обусловлено организационно-техническими или экономическими причинами и не препятствует развертыванию комплексной информационной сети вуза и внедрению унифицированных принципов безопасного доступа к информационным ресурсам.

Состояние в вузах третьего уровня архитектуры комплексной информационной сети можно охарактеризовать следующим образом: в основном завершен переход от локальных программных приложений, автоматизирующих отдельный деловой процесс и опирающихся на локальный набор данных, к корпоративным клиент-

серверным информационным системам, обеспечивающим доступ пользователей к оперативным базам данных вуза. В том или ином виде решена задача интеграции данных, порожденных различными информационными системами, что позволяет усовершенствовать бизнес-процессы, повысить качество управления и принятия решений.

Активное внедрение Интернета и новых информационных технологий в образовательный процесс и систему управления вузом создало предпосылки к появлению корпоративных сетей. Корпоративная сеть вуза – это информационная система, включающая в себя компьютеры, серверы, сетевое оборудование, средства связи и телекоммуникации, систему программного обеспечения, предназначенную для решения задач управления вузом и ведения образовательной деятельности. Корпоративная сеть обычно объединяет не только структурные подразделения вуза, но и их региональные представительства. Ранее недоступные для вуза, в настоящее время эти сети стали активно внедряться в образовательные структуры в связи с массовым распространением Интернета и его доступностью [6].

Комплексная информационная безопасность вуза – система сохранения, ограничения и авторизованного доступа к информации, содержащейся на серверах в корпоративных сетях вузов, а также передаваемая по телекоммуникационным каналам связи в системах дистанционного обучения. В более широком смысле термин «комплексная информационная безопасность вуза» включает в себя два аспекта: систему защиты интеллектуальной информационной собственности вуза от внешних и внутренних агрессивных воздействий и систему управления доступом к информации и защиты от агрессивных информационных пространств. В последнее время, в связи с неконтролируемым массовым развитием Интернета, последний аспект безопасности становится особенно актуальным.

Под термином «информационное пространство» понимается информация, содержащаяся на серверах в корпоративных сетях учебных заведений, учреждений, библиотек и в глобальной сети Интернет, на электронных носителях информации, а также передаваемая по телевизионным каналам связи или по телевидению. Агрессивное информационное пространство – это информационное пространство, содержание которого может вызвать проявления агрессии у пользователя как сразу же после информационного воздействия, так и через некоторое время (отдаленный эффект). Термин основан на гипотезе, что информация в определенных

формах и содержании может вызвать определенные эффекты с проявлением агрессии и враждебности [6].

Проблемы комплексной информационной безопасности корпоративных сетей вузов гораздо шире, разнообразнее и острее, чем в других системах. Это связано со следующими особенностями:

- корпоративная сеть вуза строится обычно на концепции «скудного финансирования» (оборудование, кадры, нелицензионное программное обеспечение);
- как правило, корпоративные сети не имеют стратегических целей развития. Это значит, что топология сетей, их техническое и программное обеспечение рассматриваются с позиций текущих задач; в одной корпоративной сети вуза решаются две основные задачи: обеспечение образовательной и научной деятельности и решение задачи управления образовательным и научным процессами. Это означает, что одновременно в этой сети работает несколько автоматизированных систем или подсистем в рамках одной системы управления.

В такой сети возможны как внутренние, так и внешние угрозы безопасности информации: попытки несанкционированного администрирования баз данных; исследование сетей, несанкционированный запуск программ по аудиту сетей; удаление информации, в том числе библиотек; запуск игровых программ; установка вирусных программ и троянских коней; попытки взлома; сканирование сетей, в том числе других организаций, через Интернет; несанкционированная откачка из Интернета нелицензионного софта и установка его на рабочие станции; попытки проникновения в системы бухгалтерского учета; поиск «дыр» в ОС, firewall, Proxy-серверах; попытки несанкционированного удаленного администрирования ОС; сканирование портов и т. п.

Источниками возможных угроз информации являются: компьютеризированные учебные аудитории, в которых проходит учебный процесс; Интернет; рабочие станции неквалифицированных в сфере информационной безопасности работников вуза. Анализ информационных рисков можно разделить на следующие этапы: классификация объектов, подлежащих защите, по важности; определение привлекательности объектов защиты для взломщиков; определение возможных угроз и вероятных каналов доступа на объекты; оценка существующих мер безопасности; определение уязвимостей в обороне и способов их ликвидации; составление ранжированного списка угроз; оценка ущерба от

несанкционированного доступа, атак в отказе обслуживании, сбоев в работе оборудования.

Основные объекты, нуждающиеся в защите от несанкционированного доступа: бухгалтерские ЛВС, данные планово-финансового отдела, а также статистические и архивные данные; серверы баз данных; консоль управления учетными записями; www/ftp-серверы; ЛВС и серверы исследовательских проектов. Как правило, связь с Интернетом осуществляется сразу по нескольким линиям связи (оптоволоконная магистраль, спутниковые и радиоканалы). Отдельные каналы предоставляются для связи с другими университетами или для безопасного обмена данными. Чтобы исключить риски, связанные с утечкой и порчей передаваемой информации, такие сети не должны подключаться к глобальным сетям и общей университетской сети. Критически важные узлы для обмена данными университета (например, бухгалтерская ЛВС) также должны существовать отдельно.

Первый рубеж обороны от атак извне – роутер (маршрутизатор). Он применяется для связи участков сети друг с другом, а также для более эффективного разделения трафика и использования альтернативных путей между узлами сети. От его настроек зависит функционирование подсетей и связь с глобальными сетями (WAN). Его главная задача в плане безопасности – защита от распределенных атак в отказе обслуживания (DDOS). Вторым рубежом может служить межсетевой экран (МСЭ): аппаратно-программный комплекс Cisco PIX Firewall. Затем следует демилитаризованная зона (DMZ). В этой зоне необходимо расположить главный прокси-сервер, dns-сервер, www/ftp, mail-серверы. Прокси-сервер обрабатывает запросы от рабочих станций учебного персонала, серверов, не подключенных напрямую к роутеру, и фильтрует трафик. Политика безопасности на этом уровне должна определяться блокированием нежелательного трафика и его экономией (фильтрация мультимедиаконтента, iso-образов, блокировка страниц нежелательного/нецензурного содержания по ключевым словам). Чтобы не происходило скачивания информации, зараженной вирусами, на этом сервере оправдано размещение антивирусных средств. Информация от прокси-сервера должна параллельно отсылаться на сервер статистики, где можно посмотреть и проанализировать деятельность пользователей в Интернете. На почтовом сервере обязательно должен присутствовать почтовый антивирус, например, Kaspersky AntiVirus for Mail servers. Так как эти серверы связаны

непосредственно с глобальной сетью, аудит программного обеспечения, установленного на них, – первоочередная задача инженера по информационной безопасности вуза. Для экономии средств и гибкости настраивания желательно применять opensource ОС и программное обеспечение.

Некоторые университеты имеют свой пул дозвона для выхода в Интернет и используют каналы связи учреждения. Во избежание использования этого доступа посторонними лицами в незаконных целях работники учебного заведения не должны разглашать телефон пула, логин, пароль. Степень защищенности сетей и серверов большинства вузов России оставляет желать лучшего. Причин тому много, но одна из главных – плохая организация мер по разработке и обеспечению политики информационной безопасности и недооценка важности этих мероприятий. Вторая проблема заключается в недостаточном финансировании закупок оборудования и внедрения новых технологий в сфере информационной безопасности.

Система комплексной информационной безопасности должна включать в себя выработку следующих политик. Прежде всего, это финансовая политика развертывания, развития и поддержания в актуальном состоянии корпоративной сети вуза. Она является доминирующей и ее можно разделить на три направления: скудное финансирование, финансирование с разумной достаточностью и приоритетное финансирование. Вторая политика определяется уровнем организации развертывания и сопровождения корпоративной сети вуза. Третья политика относится к кадровому составу информационного центра. Для вуза она особенно актуальна в связи с повышенной востребованностью опытных сисадминов. Политика программного обеспечения в настоящее время – один из затратных факторов развития корпоративной сети. Рациональные подходы к его решению в условия монопольного рынка ОС и программных продуктов Microsoft – это отдельный вопрос, требующий внимательного рассмотрения. Политика технического обеспечения, может быть, не вполне актуальна в условиях достаточного финансирования. Наконец, последняя политика связана с формирование морально-этических норм толерантного поведения в информационных системах и разумного ограничения от посещений агрессивных информационных пространств. Недооценка этих направлений будет компенсироваться повышенными финансовыми затратами на поддержание корпоративных сетей.

Библиографический список

1. Концепция национальной безопасности РФ, утверждена Указом Президента РФ от 17.12.97 г. № 1300 (в ред. Указа Президента РФ от 10.01.2000 г. № 24).

2. Доктрина информационной безопасности Российской Федерации, утверждена Президентом РФ 9.09.2000 г. Пр-1895.

3. Труфанов А. И. Политика информационной безопасности вуза как предмет исследования // Проблемы Земной цивилизации. – Вып. 9. – Иркутск: ИрГТУ, 2004 / library.istu.edu/civ/default.htm.

4. Волков А. В. Обеспечение ИБ в вузах // Информационная безопасность. 2006. № 3, 4 / http://www. itsec.ru/articles2/bepub/insec–3 + 4–2006.

5. Крюков В. В., Майоров В. С., Шахгельдян К. И. Реализация корпоративной вычислительной сети вуза на базе технологии Active Directory // Тр. Всерос. науч. конф. «Научный сервис в сети Интернет». – Новороссийск, 2002. – С. 253–255.