П.С.ПОЙТА, В.И.ДРАГАН, Б.Н.СКЛИПУС,
Д.А.КОСТЮК, А.П.ДУНЕЦ, С.С.ДЕРЕЧЕННИК

ОБЕСПЕЧЕНИЕ ИНФОРМАЦИОННОЙ БЕЗОПАСНОСТИ ПРИ ОРГАНИЗАЦИИ УЧЕБНОГО ПРОЦЕССА В РАМКАХ ЛОКАЛЬНОЙ СЕТИ УНИВЕРСИТЕТА

Одной из проблем, сопутствующих развитию современного учебного заведения, как и любой иной крупной организации, является обеспечение внутреннего информационного пространства, объединяющего вычислительные ресурсы подразделений. Технические и организационные решения, обеспечивающие функционирование локальной вычислительной сети (ЛВС), должны, помимо функций хранения и передачи информации, выполнять защиту данных и программного обеспечения компьютерного парка от различных внешних и внутренних угроз. Грамотная организация сети и выбор технологий, используемых на серверах и рабочих станциях, позволяют упростить процедуры обслуживания ЛВС и восстановления после сбоев, исключить воздействие ряда вредоносных факторов, значительно увеличить обнаруживаемость вандальных воздействий, ускорить устранение их последствий.

Нами рассмотрен подход к защитным мерам, принимаемым при организации крупной ЛВС, на примере информационно-вычислительной сети Брестского государственного технического университета (БрГТУ).

Сервисы (службы), предоставляемые пользователям в рамках ЛВС БрГТУ и в той или иной степени универсальные для высших учебных заведений, можно разделить на следующие категории [1]:

– аутентификация пользователей для работы в сети;
– хранение файлов на сетевых дисках;
– веб-хостинг (сайт университета) и электронная почта;
– предоставление доступа в Интернет с дополнительной аутентификацией и хранением статистики сетевой активности.

Можно выделить три основные роли пользователей локальной сети: студенты, преподаватели и административно-управленческий персонал.

Защита информации в рамках обеспечения учебного процесса в целом и предоставления пользователям перечисленных сервисов в частности, в свою очередь, подразделяется на следующие категории:

– физическая защита аппаратных средств;
– защита от вредоносной активности со стороны пользователей;
– защита от внешних угроз;
– защищенность резервного копирования системных и прикладных данных.

Физическая защита аппаратных средств осуществляется использованием отдельных помещений с ограниченным доступом для размещения коммутационных узлов локальной сети и серверов, что гарантирует как сохранность дорогостоящего оборудования, так и свободную работу администраторов по его настройке и профилактике. Опорная сеть (совокупность линий связи между зданиями университетского комплекса) обеспечивает однотипный доступ пользователей к необходимым информационным ресурсам, что особенно важно для университетов с их обширным компьютерным парком, размещенным в нескольких корпусах различной степени территориальной рассредоточенности. В БрГТУ для соединения зданий между собой в большинстве случаев используются оптические кабели, что обеспечивает необходимую помехозащищенность и надежность одновременного подключения большого числа компьютеров; при этом критичный участок между основными корпусами имеет резервную линию оптической связи. Однако в ситуации, когда оправдана экономия средств, используются недорогие линии связи и соответствующее оборудование:

так, расположенный в отдельном корпусе небольшой физический сегмент ЛВС из 16 точек подключен с помощью телефонной линии и модемов VDSL.

Имеющаяся в настоящее время схема маршрутизации сети БрГТУ сформирована в ходе постепенного наращивания сложности ЛВС после ее первоначального развертывания и с учетом опыта эксплуатации. В составе ЛВС выделено несколько подсетей:

– основная ЛВС университета;
– ЛВС бухгалтерии;
– защищенный сегмент, в котором находятся ректорат и приемная комиссия;
– отдельная подсеть для студенческих компьютеров в общежитиях;
– Интернет-сегмент университета;
– отдельные подсети кафедр компьютерного профиля.

Приведенное разделение выполнено с учетом требований по защищенности и необходимости оптимизации потоков передаваемых данных. В частности, наличие подсетей последнего типа позволяет кафедрам, обладающим сотрудниками надлежащей квалификации, выполнять администрирование собственного сегмента и тестировать новые подходы к организации вычислительного процесса без влияния на остальные сегменты сети [2, 3].

Защита от вредоносной активности со стороны пользователей выполняется как заданием прав доступа, ограничивающих их активность в пределах конкретных наборов действий и сегментов сети, так и разграничением сегментов сети межсетевыми экранами, блокирующими межсегментные коммуникации по любым сетевым портам кроме строго необходимых для авторизации пользователей и доступа к файл-серверу с методическими материалами и программным обеспечением. Авторизация пользователей выполняется сервером Novell, предоставляющим LDAP-базу пользовательских учетных записей. Доступ к большинству прикладных программ на рабочих станциях осуществляется через сетевую систему Novell ZENworks, благодаря чему исключена необходимость установки множества различных прикладных пакетов на рабочие станции и достигнута унификация дисковых образов последних.

В качестве недостатка применяемых мер защиты можно отметить непродолжительную пиковую загрузку сети при запуске прикладных программных пакетов, а также использование на рабочих станциях антивирусного пакета AVP 6-й корпоративной версии, оказывающей заметный негативный эффект на производительность рабочей станции. Для усиления защиты на рабочих станциях учебных классов отключены сменные флеш-накопители, из конфигураций рабочих станций исключены DVD-приводы, а содержимое активных разделов жесткого диска возвращается к исходному состоянию при каждой перезагрузке с помощью специально модифицированной версии операционной системы.

В подсетях кафедр компьютерного профиля перечисленные ограничения рабочих станций сняты – взамен дополнительных мер контроля сетевого трафика на шлюзах, соединяющих их с основной ЛВС. Снятие указанных выше локальных ограничений вызвано, в первую очередь, требованиями учебного процесса, т. к. в рамках ряда дисциплин, изучаемых специалистами компьютерного профиля, требуется предоставить студентам более полный доступ к аппаратной подсистеме рабочих станций и сетевых коммуникаций [2, 4]. Кроме того, в рамках подсети кафедры электронных вычислительных машин и систем действует специализированная лаборатория для изучения аппаратно-программных систем защиты информации. Лаборатория оснащена комплектом средств «Аккорд NT/2000», «Аккорд – РАУ» и «Шипка–1.6», предоставленных университету в 2009 году ОКБ «САПР» и Всероссийским НИИ проблем вычислительной техники и информатизации в рамках Соглашения о научно-техническом сотрудничестве. Практикумы, выполняемые студентами в данной лаборатории, также являются причиной модификаций политики администрирования рабочих станций кафедры.

На серверах ЛВС, предоставляющих услуги электронной почты и веб-доступа внутренним пользователям и пользователям из сети Интернет, применяются дополнительные меры защиты от вандальных воздействий. Внешняя защита обеспечивается настройками межсетевых экранов и мониторингом вирусной активности, а для доступа локальных пользователей сети к внешним ресурсам используется наложенная частная сеть (VPN).

Сеть VPN функционирует поверх существующей инфраструктуры ЛВС университета, обеспечивая доступ к сети Интернет для сотрудников и студентов университета с учетом требований защищенности передаваемой информации и вопросов безопасности пользования соответствующими услугами. Учитывая обширность компьютерного парка, для разделения нагрузки в рамках ЛВС для различных сегментов сети применено четыре сервера VPN-доступа. Данные сервера работают под управлением Debian Linux, а защищенную авторизацию пользователей для доступа к Интернет централизованно выполняет пакет FreeRADIUS, установленный на одном из серверов. Журналирование сетевой активности выполняется с использованием мощной СУБД и соответствующего сервера с большим дисковым массивом, что позволяет в случае возникновения чрезвычайной ситуации выяснить время недопустимых сетевых действий, локализовать использованный для их осуществления компьютер и пользователя, учетная запись которого была при этом задействована. Для минимизации вероятности работы пользователей под чужими учетными записями на сервере введены: запрет на одновременный вход на нескольких компьютерах и обязательное требование периодической смены пароля.

Частью системы обеспечения бесперебойной работы ЛВС является проведение регулярного резервного копирования системных и прикладных данных. В рамках ЛВС наблюдается большое разнообразие типов оборудования, программного обеспечения (в т.ч. серверных операционных систем), данных различных типов, что порождает большой перечень требуемых процедур резервного копирования и их разнородность. Информация на серверах сети преимущественно хранится в RAID-массивах; кроме того, в рамках ЛВС выделены два сервера под управлением Windows 2003, выполняющие автоматизированную архивацию данных. Резервное копирование в ЛВС университета осуществляется для многих сервисов корректно и в достаточном объеме; однако вместо использования стандартных средств резервирования на ряде серверов в настоящий момент применяются ручные процедуры либо автоматизация посредством нестандартизированных программных средств собственной разработки.

Приведенный комплекс мер и программно-аппаратных решений позволяет обеспечить достаточный уровень безопасности и устойчивости к возможной случайной или умышленной вредоносной активности, несмотря на территориальную распределенность, исторически сложившуюся многокомпонентную гетерогенную архитектуру информационно-вычислительной сети и значительное расхождение в требованиях и подходах к эксплуатации компьютерного парка среди подразделений университета.

Литература

1. П.С. Пойта, В.И. Драган, А.П. Дунец, Д.А. Костюк, В.И. Хведчук, С.С. Дереченник. Подход к модернизации гетерогенной сетевой инфраструктуры на примере информационно-вычислительной сети университета // Вестник БрГТУ. – 2010. – №5: Физика, математика, информатика. – С. 75–78.

2. Б.Н. Склипус, С.С. Дереченник, А.А. Склипус. Универсальный реконфигурируемый микропроцессорный стенд для лабораторных занятий / Проблемы проектирования и производства РЭС: сб. материалов V международной НТК (Новополоцк, Май 29–30, 2008). – Т. III, Информатика. – Р. 233–237.

3. Д.А. Костюк, Р.В. Сченснович. Использование в образовательном процессе вычислительных сетей на базе Windows Server 2008 // Информационные технологии в

образовании: материалы Международной научно-практической конференции, 21–22 мая 2009. / БНТУ. – Минск, 2009. – С. 109–113.

4. Д.А. Костюк. Изучение низкоуровневого программирования и вычислительной ой архитектуры на базе платформы GNU/Linux // Свободное программное обеспечение в высшей школе: тезисы докладов 5-й конференции (Переславль-Залесский, 30–31 января 2010 г.). - М.: Институт логики, 2010. – С. 32–35.

А.В.ПУГАЧ

ИСПОЛЬЗОВАНИЕ ПРОФИЛЕЙ ЗАЩИТЫ ПРИ ПРОЕКТИРОВАНИИ СИСТЕМ ЗАЩИТЫ АВТОМАТИЗИРОВАННЫХ СИСТЕМ

Информация, содержащаяся в продуктах или системах информационных технологий (далее – ИТ), является важнейшим ресурсом, позволяющим организациям успешно выполнять их функции. В системах ИТ может находиться также информация, отнесенная к государственным секретам или информация, критичная к сохранению своих свойств. Продукты или системы ИТ такого рода должны выполнять свои функции при соответствующих гарантиях защиты информации от несанкционированного доступа, изменения или потери.

Значительным шагом вперед в решении проблем безопасности продуктов и систем ИТ (к которым относятся автоматизированные системы (далее - АС), в том числе и специального назначения) явилось введение в действие стандартов [1]–[3], которые определяют структуру и содержание двух документов – профиль защиты (далее – ПЗ) и задание по безопасности (далее – ЗБ) и содержат библиотеку требований, которые выбираются и включаются в ПЗ и ЗБ. С одной стороны, ПЗ может рассматриваться как детальное определение требований безопасности и гарантий, которые пользователи хотят видеть в продукте или системе ИТ. ПЗ – независимая от реализации структура для определения и обоснования требований безопасности, представляющая собой набор задач безопасности, функциональных и гарантийных требований. ПЗ разрабатывается для новых продуктов и систем. С другой, ЗБ может рассматриваться как описание в терминах требований безопасности того, что предлагает разработчик.

Главная задача ПЗ и ЗБ – создание основы для взаимодействия между потребителями (заказчиками), производителями и экспертами по сертификации продуктов и систем ИТ по требованиям безопасности. Каждая из этих сторон имеет свои интересы и взгляды на проблемы информационной безопасности.

Потребители заинтересованы, во-первых, в методике, позволяющей обоснованно выбрать продукты, отвечающие их потребностям, для чего им необходима шкала оценки безопасности ИТ, во-вторых, нуждаются в инструменте, с помощью которого они могли бы формулировать свои требования производителям. При этом потребителям важны характеристики и свойства конечного продукта. С этой точки зрения шкала оценки безопасности выглядит следующим образом:

Уровень 1. Система для обработки общедоступной информации, критичной к сохранению, например, свойств целостности и доступности информации.

Уровень 2. Система для обработки информации ограниченного распространения, например, с грифом не выше «для служебного пользования», и т. д.

Производители, в свою очередь, нуждаются в инструментах для сравнения возможностей своих продуктов, в применении процедуры сертификации для объективной оценки их свойств, а также в стандартизации набора требований безопасности. С точки зрения производителя, требования безопасности должны быть максимально конкретными и