

Создание слайд - лекции по “Начертательной геометрии” требует от авторов не только хорошего знания теоретического материала, но и умения работать в программах PowerPoint, Word, AutoCAD, CorelDraw и т. д.

Для воспитания и обучения, востребованных обществом специалистов, необходимо чтобы занятия проводились высоко квалифицированными преподавателями с использованием новых информационных технологий.

**Климов В.Г.**

## **МЕТОДОЛОГИЯ ЗАЩИТЫ ОБРАЗОВАТЕЛЬНОЙ И НАУЧНОЙ ИНФОРМАЦИИ В НАСТОЛЬНЫХ КОМПЬЮТЕРНЫХ СИСТЕМАХ ПРОФЕССИОНАЛЬНЫХ УЧЕБНЫХ ЗАВЕДЕНИЙ**

*vklimov@perm.ru*

*Пермский государственный университет (ПГУ)*

*г. Пермь*

В условиях широкого внедрения в педагогическую деятельность информационных и телекоммуникационных технологий обучения современные системы безопасности предлагают все более совершенные методы защиты образовательных локальных сетей от различных типов угроз. Однако в них не уделяется достаточного внимания таким уязвимым элементам инфраструктуры профессиональных учебных заведений, как настольные компьютерные системы. Причем обычно недооценивается не только опасная способность враждебных программных кодов мгновенно распространяться по электронной почте, через Интернет и системы совместного использования файлов, но и та роль, которую играют в этом неправильные и неумелые действия преподавателей и студентов. А ведь в состав локальной сети профессионального учебного заведения могут входить сотни ноутбуков и настольных компьютеров.

Противоречивость современной образовательной и научной сферы информационной безопасности состоит в том, что основной упор в ней делается на защиту периметра и внутренней инфраструктуры сети, несмотря на то, что по статистике наиболее уязвимыми узлами сети являются рабочие станции и мобильные компьютеры, на которых обрабатывается большой объем научной и образовательной конфиденциальной информации и хранится интеллектуальная собственность профессионального учебного заведения. Именно они - самое критичное место в построении защиты информационных сетей, так как подвержены угрозам, исходящим как извне, так и от легальных пользователей сети.

### *Фазы жизни*

Рассматривая угрозы настольным компьютерным системам, важно понимать, что для того, чтобы какая-либо атака была успешной, она должна пройти три жизненные фазы: проникновение, выполнение, распространение. Например, проникновение может быть осуществлено различными методами - посредством электронной почты, через Web-браузер, за счет удаленного переполнения буфера памяти и т.п. Выполнение - это запуск злонамеренного кода, уже загруженного вследствие успешно пройденной первой фазы. Распространение означает компрометацию других ресурсов, составляющих объект атаки, или иных узлов сети - как посредством удаленного управления, так и в автономном режиме.

### *Двухвекторная модель атак*

Структуру угроз настольным образовательным и научным компьютерным системам можно представить с помощью двухвекторной модели их возникновения - угрозы атак на уровне сети и угрозы атак на уровне приложений. На сетевом уровне угрозу составляют в себе DoS-атаки и Интернет-черви, на уровне приложений - различные вирусы, E-mail-черви, троянские программы, шпионское программное обеспечение и т.д. В этом свете рабочие станции и мобильные компьютеры приобретают значение важнейшего участка информационной защиты - первого и последнего рубежа обороны. Первым рубежом они являются относительно действий зарегистрированных пользователей, а последним рубежом, конечной точкой, целью - для внешних злоумышленников.

Атаки сетевого уровня (network-based attacks) могут протекать без какого-либо участия пользователя. Они становятся возможными из-за наличия уязвимостей в различных сетевых протоколах и службах. Использование данных уязвимостей реализуется посредством прямого взлома и воровства в информационных сетях, распространения сетевых червей, различных атак типа "отказ в обслуживании" (DoS-атаки), установки разнообразных программ, результатом действия которых является появление у злоумышленника путей обхода системы защиты (backdoors) и возможности удаленно управлять узлом сети (footholds). Но этим многообразие видов сетевых атак не ограничивается: есть еще множество различных путей для использования уязвимостей сетевого уровня.

### *Методология защиты от сетевых атак*

Какие же защитные технологии можно противопоставить постоянно эволюционирующим атакам на двух основных векторах угроз? Рассмотрим сначала вектор сетевых атак.

Повсеместное использование межсетевых экранов и антивирусных средств является необходимой, но сегодня - явно не достаточной мерой защиты образовательной и научной информации в российских профессиональных учебных заведениях. Эти две хорошо зарекомендовавшие себя технологии имеют как достоинства, так и недостатки. А в связи со стремительным развитием угроз информационной безопасности средства защиты, использующие эти технологии разрозненно, сами зачастую становятся объектом атаки.

Поэтому на сетевом уровне защиту рабочих станций и мобильных компьютеров, которая обеспечивается, как правило, персональным межсетевым экраном, необходимо дополнить системой предотвращения атак и системой защиты памяти или системой предотвращения атак типа "переполнения буфера".

#### *Personal Firewall*

Персональный межсетевой экран (Personal Firewall, PFW) - наиболее распространенная и понятная форма защиты настольных компьютерных систем для подавляющего числа преподавателей и студентов. Благодаря набору правил фильтрации пакетов PFW может уменьшить, но не ликвидировать риск того, что компьютер подвергнется нападению из внешней сети. Путем блокирования доступа к портам, IP-адресам, сетевым протоколам и службам PFW-технология может предотвращать только небольшое число хорошо известных атак (SYNFlood, IPspoofing, Ping of Death, WinNuke и т.д.). Несмотря на свои бесспорные достоинства, технологии межсетевого экранирования не справляются с новыми, постоянно развивающимися угрозами, примерами реализации которых можно назвать известные всем атаки: Nimda, Code Red, Slammer и т.д.

#### *IDS и IPS*

Получившая широкое распространение технология обнаружения атак (Intrusion Detection System, IDS) использует глубокий анализ пакетов сетевого трафика, прошедшего через правила фильтрации межсетевого экрана, для извещения пользователя о попытке атаки на информационную систему. Появившись совсем недавно, технология IDS достаточно быстро переросла в технологию защиты следующего поколения - предотвращение атак (Intrusion Prevention System, IPS). По сути дела, IPS стала результатом объединения функциональных возможностей IDS и систем межсетевого экранирования. Механизм обнаружения атак, как правило, основан на сигнатурных методах анализа пакетов и методах анализа протоколов.

Сигнатурные методы (сравнение реального трафика с шаблоном атаки) эффективны для обнаружения уже известных атак и практически беззащитны перед неизвестными атаками. В свою очередь, методы анализа протоколов обладают потенциалом для обнаружения неизвестных атак и сетевых червей, но имеют недостаток - большое потребление ресурсов при обнаружении атак в реальном времени. Анализ протоколов включает в себя использование целого ряда методик: поведенческого анализа, сравнения структуры и содержания пакетов на соответствие RFC (Request for Comments) и т.д. Предотвращение, в данном случае, возможно только для известных и неизвестных атак, направленных на уже известные уязвимости. Поэтому необходим еще один уровень защиты, предотвращающий атаки на неизвестные уязвимости.

#### *BOEP*

Система защиты от "переполнения буфера" (Buffer Overflow Exploit Prevention, BOEP) - одна из новейших технологий обеспечения безопасности настольных компьютерных систем образовательного и научного назначения. Она предотвращает исполнение вредоносного кода, использующего атаки типа "переполнения буфера". По статистике исследовательской лаборатории X-Force, такие атаки сейчас наиболее распространены. Их доля составляет до 80% от общего числа атак. Основа этих атак - принцип функционирования операционных систем, где программа получает привилегии и права запустившего ее пользователя или процесса. Атака заключается в том, что в каком-либо месте программы происходит копирование данных из одного участка памяти в другой без проверки того, достаточно ли для них места там, куда их копируют. Область памяти, куда копируются данные, принято называть буфером. Таким образом, если данных слишком много, то часть их попадает за границы буфера - происходит "переполнение буфера". Если злоумышленнику удастся организовать переполнение буфера, он может удаленно выполнять команды на машине-жертве с правами атакованного приложения - того приложения, в котором обычный пользователь сети получает частичный или полный контроль над этим хостом, например, запуск командной оболочки с правами администратора. "Бессигнатурная" технология BOEP позволяет защититься от подавляющего числа уже известных атак и делает невозможными дальнейшие попытки использовать такого рода уязвимости, т.е. защищает от неизвестных атак.

Технология BOEP стоит на последней линии обороны от сетевых атак. Персональный межсетевой экран предотвращает известные и неизвестные атаки против сетевых сервисов и служб, не задействованных пользователем. Система IPS блокирует известные и неизвестные атаки, которые используют уже известные уязвимости. И, наконец, BOEP реализует защиту от атак, основанных на неизвестных уязвимостях.

#### *Методика защиты на уровне приложений*

Защитившись от атак, которые мы отображаем с помощью сетевого вектора, обратим свое внимание на угрозы от атак, идущих по вектору приложений. Антивирусные программы, которые сегодня повсеместно защищают рабочие станции и мобильные компьютеры образовательного и научного назначения на уровне приложений, не справляются с нарастающим валом современных атак. Поэтому можно говорить о необходимости дополнения антивирусных средств новыми технологиями, такими как предотвращение вирусных атак и контроль действий приложений. Рассмотрим все три технологии подробнее.

#### *Antivirus*

Антивирусные системы - наиболее распространенные средства защиты настольных компьютерных систем, которые используются в начальной фазе жизненного цикла атаки. Традиционные антивирусные продукты эффективны в обнаружении и предотвращении известных вирусов, червей и некоторых троянских программ. Продуктивность этой технологии напрямую зависит от скорости выпуска производителем вирусных сигнатур. Как правило, время выхода сигнатуры для нового вируса составляет до 24 часов с момента его

обнаружения. Любая трансформация кода ведет к появлению нового вируса, для обнаружения и предотвращения которого нужна, опять же, новая сигнатура. Зависимость этого вида защиты от того, насколько быстро появляются сигнатуры новых вирусов, обуславливает потребность в средствах защиты от неизвестных вирусов.

#### *Virus Prevention System*

Технология предотвращения вирусных атак (Virus Prevention System, VPS), в отличие от традиционных антивирусных средств, решает проблему борьбы с неизвестными вирусами. Это технология следующего поколения, которая дополняет обычные антивирусные механизмы и анализирует поведение программ до их выполнения в образовательной или научной информационной системе на предмет обнаружения и блокирования враждебных действий.

Использование данной технологии не зависит от появления новых сигнатур и поэтому не является реактивным процессом. Анализ поведения программ проводится в виртуальной среде, никаким образом не связанной с информационной системой, до их выполнения. Так как вирусы пишутся с использованием ограниченного количества достаточно известных методик, то обнаружить проявления аномального поведения программы не составляет никакого труда.

#### *Application Control*

Следующий рубеж защиты обеспечивает технология контроля деятельности приложений (Application Control, AC), завершающая линейку средств информационной защиты уровня приложений. Технология AC может предотвращать атаки в фазе их выполнения или раньше. Механизм AC, как и PFW, основан на регулировании политики безопасности в образовательной среде путем создания списка разрешенных на запуск приложений (замкнутая программная среда) и ограничения прав доступа приложений (различного типа, включая различные приложения P2P) на обращение к корпоративной сети учебного заведения. Кроме того, с помощью AC можно проверять пользовательскую систему на наличие установленных обновлений ОС и антивирусных средств. Несмотря на достоинства этой технологии, ее использование будет иметь эффект только в случае ее использования совместно с другими защитными технологиями, но не в качестве единственного средства защиты.

#### *Выводы*

Сегодня все ведущие производители средств информационной безопасности предлагают свои решения для защиты образовательных и научных настольных компьютерных систем. Это такие продукты, как Symantec Client Security компании Symantec Corporation, Cisco Security Agent от Cisco Systems и Proventia Desktop - решение компании Internet Security Systems (ISS), за которое она была удостоена награды 2005 Frost & Sullivan Award "За лидерство в технологиях" в категории "Защита рабочих станций". Все эти системы, так или иначе, выводят комплексную многоуровневую защиту рабочих станций и мобильных компьютеров на новую ступень развития и реализуют современный подход к безопасности конечного пользователя с применением всей гаммы защитных технологий.

По нашему мнению, профессиональные учебные заведения России (начальные, средние и высшие) должны реально осознавать необходимость активной защиты настольных компьютерных систем от широкого спектра прогрессирующих современных угроз информационной безопасности. Выделение двух основных векторов атак облегчает понимание роли и перспектив различных технологий защиты образовательной и научной информации. Кроме того, важно знать, что может и что не может делать каждая отдельно взятая технология защиты. Только совместное использование средств периметровой и шлюзовой защиты с механизмами защиты настольных компьютерных систем позволит выстроить эффективную, эшелонированную оборону в учебных заведениях профессионального образования против постоянно эволюционирующих современных угроз.

**Костиков А.Н.**

**ВЫЯВЛЕНИЕ ИСХОДНЫХ ПУТЕЙ И МЕТОДОВ РЕШЕНИЯ ПРОБЛЕМЫ ПОВЫШЕНИЯ ПРОФЕССИОНАЛЬНОЙ ПОДГОТОВКИ ПРЕПОДАВАТЕЛЯ ВЫСШЕЙ ШКОЛЫ В ОБЛАСТИ ДИСТАНЦИОННЫХ ТЕХНОЛОГИЙ ОБУЧЕНИЯ В ОТЕЧЕСТВЕННОМ ПОСЛЕДИПЛОМНОМ ОБРАЗОВАНИИ**

---

*kostikov@clipsal.ru*

*Российский государственный педагогический университет им. А.И. Герцена (РГПУ им. А.И. Герцена)  
Санкт-Петербург*

Успешное реформирование высшей школы связано непосредственно с ее главным, стратегическим направлением - подготовкой научно-педагогических кадров. От их научной квалификации, профессионально-педагогической компетенции, в первую очередь, зависит формирование нового поколения специалистов - образованных, воспитанных, с высоким уровнем общей и профессиональной культуры, интеллектуального развития, конкурентоспособности к активной профессиональной и социальной деятельности в изменившихся социально-экономических условиях. Отечественная высшая школа накоплен значительный опыт подготовки научно-педагогических кадров через аспирантуру, докторантуру, ФПК, стажировку. Однако эти формы подготовки в основном ориентированы на предметную область знаний и очень слабо - на использование информационных технологий в своей предметной области.