*УДК 551.482.1*

*А.Е. Шавкун, Б.П. Овечкин*

# СИСТЕМА ОБЕСПЕЧЕНИЯ БЕЗОПАСНОСТИ КОМПЬЮТЕРНОЙ СЕТИ ВУЗА

Бурный рост Internet-технологий, новые технологии поиска и отображения данных в Internet, а также коммерциализация этой сети делают ее все более привлекательной для различных групп пользователей, начиная с крупных организаций и заканчивая физическими лицами. Однако в дополнение к уже имеющимся обязанностям администрирования сети возникает целый спектр новых проблем: как защитить корпоративную сеть от несанкционированного доступа извне; как скрыть информацию о структуре своей сети и ее компонентов от внешних пользователей; какими средствами разграничить права доступа внешних пользователей, обращающихся к FTP, WWW-серверам, а также и своих пользователей, запрашивающих сервисы сети. Крупные сети крупных организаций (к которым относятся и сети вузов) часто подвергаются посягательствам на безопасность, но специфика этих корпоративных сетей заключается в том, что большинство таких атак происходит изнутри.

Для построения защищенной компьютерной сети необходимо проанализировать и выявить ее специфику и топологию. Без такого анализа, применяя лишь стандартные средства обеспечения безопасности, не получится полноценной системы безопасности. Компьютерная сеть вуза имеет достаточно специфическую структуру, которая определяется следующими свойствами:

- *гетерогенность*, т.е. в сети функционируют различные операционные системы (UNIX, Windows 95/NT, NetWare), которые используют различные сетевые протоколы для передачи данных по сети;
- *распределенность*, т.е. пользователь такой сети может зайти в сеть практически с любой ее точки;
- *открытость*, т.е. данные, которые выставляются в такой сети, носят обычно научно-образовательный характер и не являются какой-либо коммерческой либо сверхсекретной информацией.

С другой стороны, необходимо защитить внутренний документооборот в сети как от внешних посягательств, так и от внутренних.

Необходимо построить *систему безопасности,* т.е. комплекс программных, аппаратных и административных средств защиты. Используя стандартные сервисы обеспечения безопасности (идентификация и аутентификация, управление доступом, протоколирование и аудит, криптография, экранирование), система обеспечила бы выполнение основных составляющих информационной безопасности:

- *конфиденциальность* – защита от несанкционированного получения информации;
- *целостность* – защита от несанкционированного изменения информации;
- *доступность* – защита от несанкционированного удержания информации и ресурсов.

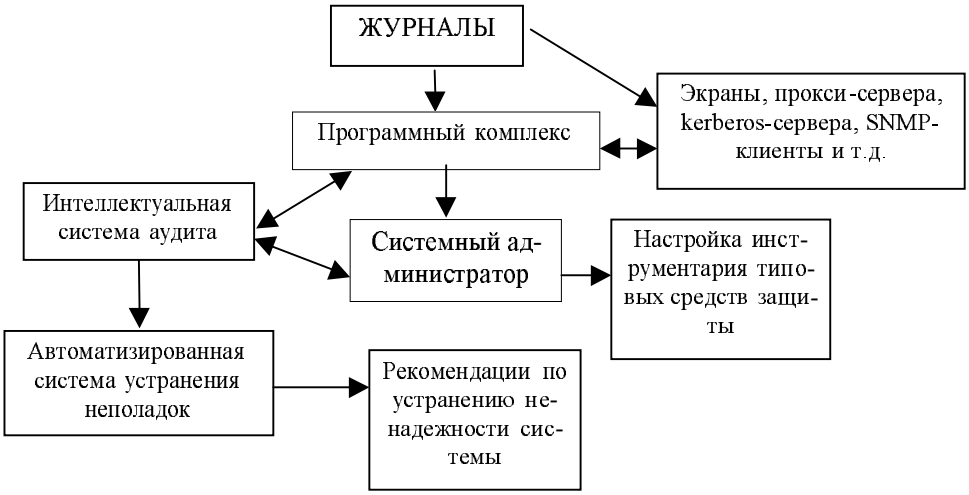
Рекомендуя какие-либо средства защиты, прежде всего необходимо помнить такое соотношение: безопасность = 1/удобство, т.е. чем безопаснее система, тем хуже живется пользователю. Политику безопасности надо вести умеренно и аккуратно.

Решая задачу построения системы безопасности, можно выделить несколько этапов:

- выявить критичные, с точки зрения безопасности, места сети вуза;
- выбрать средства защиты, особенно необходимые для структуры корпоративной сети вуза;
- дать рекомендации по их применению.

Корпоративная сеть АГУ является типовой для сетей любого крупного вуза, поэтому можно применять систему безопасности сети АГУ и в любых сетях других вузов.

Принципиальная схема основных элементов системы безопасности представлена на рисунке.




Принципиальная схема основных элементов системы безопасности

Направление стрелок на рисунке указывает на направление движения потоков данных. Данная схема требует небольших пояснений. Одна из основных компонент построенной системы безопасности – это программный комплекс, который взаимодействует со всеми субъектами (журналы, экраны, прокси-серверы, и т.д.). Программный комплекс обрабатывает поступающую информацию и либо направляет ее в интеллектуальную систему, либо выдает отчет системному оператору. Информационные потоки интеллектуальной системы идут в обоих направлениях, т.е. она может как принимать данные от программного комплекса и администратора, так и выдавать отчеты этим субъектам системы. Автоматизированная система устранения неполадок, основываясь на данных, полученных от системы аудита, автоматически выполняет действия по устранению этих проблем и выдает отчет о выполненных действиях. Некоторой проблемой в реализации такой схемы является построение достаточно интеллектуальной системы аудита, т.е. реализация алгоритма искусственного интеллекта, но для анализа каких-либо структурированных данных (которые исходят из программного комплекса) такую систему построить можно.

На данный момент в предложенной системе безопасности реализованы следующие компоненты:

- накопление данных в журналах регистрации;
- программный комплекс, который обрабатывает журналы наиболее важных сервисов (почтовый журнал, журнал учета трафика, on-line журнал).

Интеллектуальная система аудита – наиболее сложный элемент системы находится в стадии разработки. Естественно, что система безопасности может использовать типовые средства информационной защиты, например экраны – типовое средство, позволяющее разделять два множества информационных систем. Обычно экран не является симметричным, для него определены понятия «внутри» и «снаружи». При этом задача экранирования формулируется как защита внутренней области от потенциально враждебной внешней. Экранирование дает возможность контролировать также информационные потоки, направленные во внешнюю область, что способствует поддержанию режима *конфиденциальности*. Причем программных продуктов, которые реализуют данное средство, достаточно много. В АГУ используются возможности экранирования в программно-аппаратном маршрутизаторе фирмы Cisco.

Получить несанкционированный доступ к компьютеру, работающему в сети, иногда бывает достаточно легко. Такие тривиальные просчеты, как передача паролей по сети

в чистом виде, сводят на нет любую защиту. Система Kerberos ориентированна на задачи обеспечения защиты в сетях.

Kerberos – это система аутентификации, средство, обеспечивающее гарантию того, что пользователи и службы на самом деле являются теми, за кого себя выдают. Механизм обеспечения безопасности в этой системе основан на шифровании, используя алгоритм шифрования DES, Kerberos создает наборы идентификаторов, называемых «билетами». Билеты передаются по сети с целью подтверждения личности пользователя и предоставления ему доступа к сетевым службам. Эта система обеспечивает эффективную защиту паролей, при этом пользователь избавляется от необходимости вводить их каждые несколько минут. Kerberos широко используется в центральном узле связи АГУ.

Регулярное создание резервных копий данных является неотъемлемым компонентом любого плана обеспечения безопасности. Необходимо вести четкую политику резервного копирования хотя бы основных узлов сети. Это поможет в случае нарушения работоспособности системы, быстро восстановить ее. В университете резервное копирование происходит регулярно, и все основные данные серверов резервируются.

Работа над дальнейшей реализацией системы безопасности продолжается, и для обеспечения полной безопасности применения только стандартных (типовых) средств недостаточно, поэтому необходима разработка собственного программного обеспечения, а также применение некоторых организационных мероприятий.

Представленная система безопасности успешно работает, но ее эффективность зависит от усилий не одного подразделения, а от усилий всех подразделений АГУ и выполнения ими правил работы в сети.