ISBN 978-5-901795-13-2 ПРОГРАММНЫЕ СИСТЕМЫ: ТЕОРИЯ И ПРИЛОЖЕНИЯ. Переславль-Залесский, 2008

А. С. Шалауров

Разработка системы информационной безопасности компьютерной сети «Университета города Переславля» им. А. К. Айламазяна[*)]

Научный руководитель: ст. преп. Л. В. Парменова

Аннотация. Данная работа посвящена разработке системы информационной безопасности компьютерной сети «Университета города Переславля» им. А. К. Айламазяна. Разработка системы обусловлена все более обостряющейся ситуацией в области информационной безопасности и направлена на улучшение уровня защищенности как отдельных объектов, так и компьютерной сети в целом.

1. Введение

Проблема информационной компьютерной безопасности не нова — специалисты занимаются ею с того времени, как компьютер начал обрабатывать данные, ценность которых высока для пользователя. Однако за последние годы в связи с развитием сетей, ростом спроса на электронные услуги ситуация в сфере информационной безопасности серьезно обострилась, а вопрос обеспечения безопасности информации стал приоритетным для многих организаций и компаний.

Проблема информационной безопасности не обошла стороной и образовательные учреждения, информационные системы которых содержат большие объемы конфиденциальной информации по персоналу и обучающимся, нормативные документы и документы по образовательному процессу. Кроме того, для образовательных учреждений стали велики риски сетевых угроз и угроз срыва образовательного процесса из-за вывода из строя компонент информационной системы.

Данная работа направлена на разработку комплекса мер по повышению уровня информационной безопасности компьютерной сети

[*)] Представлено по тематике: *Компьютерные сети и телекоммуникации.*

«Университета города Переславля» им. А. К. Айламазяна[1], информационная система которого оказалась беззащитна перед внешними и внутренними угрозами. Разрабатываемые методы будут реализовываться исключительно для Windows компьютерной сети, так как в Университете активно развиваются Windows технологии и все больше требуют соответствующей защиты.

1.1. Целесообразность и актуальность работы

На момент начала данной работы компьютерная сеть «Университета города Переславля» им. А. К. Айламазяна была достаточно развита, но мер по защите компьютерной техники, предотвращению угроз информации и снижению рисков от угроз выработано не было. Именно поэтому риски потери информации, несанкционированного доступа к конфиденциальным документам, вывода из строя компьютерной техники, и, как следствие, срыва работы организации, были достаточно велики. Кроме того, бурное развитие информационных технологий требовало принятия адекватных мер по защите информации, средств ее обработки и хранения.

Как и во многих организациях, в «Университете города Переславля» им. А. К. Айламазяна используется антивирусное программное обеспечение, а также на некоторых компонентах структуры применяется принцип «минимально необходимых прав доступа». Кроме того, имеется неплохая серверная база, но всего этого явно не хватает для безопасного функционирования организации. В связи с этим вопрос обеспечения информационно–компьютерной безопасности данной организации становится все более актуальным и требует скорейшего решения.

1.2. Цели и задачи

Главной целью системы информационной безопасности является обеспечение устойчивого функционирования организации, предотвращение угроз ее безопасности, защита законных интересов организации от противоправных посягательств, недопущение хищения, разглашения, утраты, утечки, искажения и уничтожения информации,

[1]Сайт образовательного учреждения — http://u.pereslavl.ru/

обеспечение нормальной производственной деятельности всех ее подразделений, а так же повышение существующего уровня информационной безопасности «Университета города Переславля» им. А. К. Айламазяна.

Достижение заданных целей возможно в ходе решения следующих основных задач:

(1) отнесение информации к категории ограниченного доступа — определение важной информации, ограничение доступа к ней;
(2) своевременное выявление угроз безопасности информационным ресурсам, причин и условий, способствующих нанесению ущерба — разработка политики аудита безопасности, настройка протоколирования событий и ведения логов системы;
(3) создание условий функционирования с наименьшей вероятностью реализации угроз безопасности информационным ресурсам и нанесения различных видов ущерба — повсеместное внедрение принципа минимально допустимых пользовательских прав, ограничение доступа к особо важным компонентам системы, разработка групповых политик для разных типов пользователей;
(4) создание механизма и условий оперативного реагирования на угрозы информационной безопасности и проявления негативных тенденций в функционировании, эффективное пресечение посягательств на ресурсы — назначение администратора безопасности из числа сотрудников Группы компьютерной поддержки, отладка системы антивирусной защиты рабочих станций и серверов, ограничение сетевого доступа;
(5) создание условий для максимально возможного возмещения и локализации ущерба, наносимого неправомерными действиями, ослабление негативного влияния последствий нарушения информационной безопасности на функционирование организации — децентрализация информационных ресурсов, разработка backup–политики, подход к информационной безопасности на уровне отдельных серверных приложений[1–3].

1.3. Определение требований к системе информационной безопасности

Разрабатываемая система информационной безопасности должна удовлетворять следующим требованиям:

- Система защиты информации должна быть представлена как нечто целое; целостность системы будет выражаться в наличии единой цели ее функционирования, информационных связей между элементами системы, иерархичности построения подсистемы управления системой защиты информации;
- Система защиты информации должна обеспечивать безопасность информации, средств информации, защиту интересов участников информационных отношений и невозможность несанкционированного доступа злоумышленника к защищаемой информации;
- Система защиты информации в целом, применяемые методы и средства защиты должны быть по возможности прозрачными для законного пользователя, не создавать ему больших дополнительных неудобств, связанных с процедурами доступа к информации.

1.4. Стадии разработки системы безопасности

Разработка системы состоит из трех этапов:

(1) Первая стадия:
   - определение состава средств информационной системы;
   - анализ уязвимых элементов ИС и связанных с ними угроз;
   - анализ рисков (прогнозирование возможных потерь и последствий, вызванных существующими угрозами);

(2) Вторая стадия — определение способов защиты:
   - устраняемые угрозы;
   - защищаемые ресурсы;
   - средства защиты системы;

(3) Третья стадия — определение функций, процедур и средств безопасности, реализуемых в виде некоторых механизмов защиты.

На первой стадии для построения сбалансированной системы информационной безопасности, предполагается провести аудит существующей системы, определить компоненты информационной системы. Так же необходимо провести анализ существующих уязвимых элементов, угроз, вызванных уязвимостями и рисков в области информационной безопасности.

На второй стадии необходимо определить оптимальный уровень риска, устраняемые в рамках системы информационной безопасности угрозы, важные ресурсы и средства защиты информации.

На третьей стадии необходимо разработать и реализовать конкретные методы и средства защиты для безопасного функционирования организации. Систему информационной безопасности (контрмеры) предстоит построить таким образом, чтобы достичь заданного уровня риска.

2. Аудит информационной безопасности компьютерной сети Университета

2.1. Определение состава средств информационной системы (ИС)

Любая система информационной безопасности является частью общей информационной системы (ИС) организации и существует в рамках этой ИС. И перед тем, как приступить к разработке системы информационной безопасности, необходимо ознакомиться со всеми компонентами ИС и схемой их взаимодействия.

На рисунке 1 представлена топологическая структура компьютерной сети «Университета города Переславля» им. А. К. Айламазяна с позиции компонент ИС. Исходя из данной топологии, можно выделить три основные особенности компьютерной сети Университета:

(1) единый домен TRUBEZH (на 1й и 2й корпуса);
(2) 2 подсети 248-я и 249-я;
(3) 3 типа компьютеров (серверы, рабочие станции для занятий студентов и рабочие станции персонала).

Основными информационными ресурсами и сервисами компьютерной сети Университета являются:

(1) доменный контроллер Shark2, его функции:
    - глобальный каталог домена;

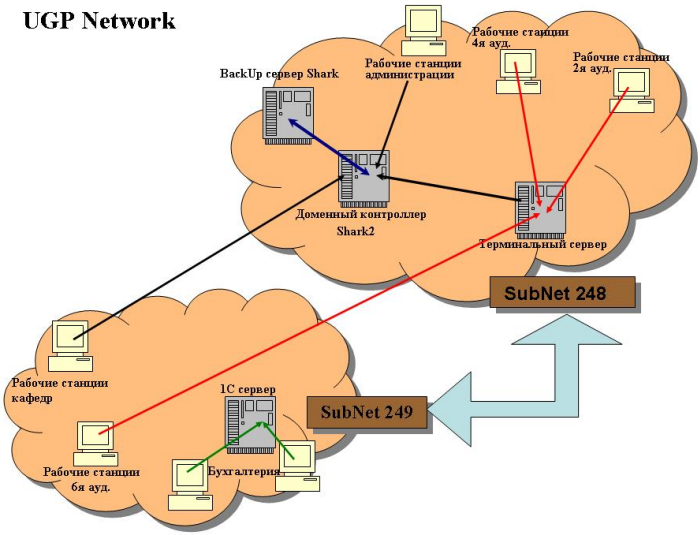

Рис. 1. Топологическая структура компьютерной сети Университета

- DNS-сервер;
- DHCP-сервер;
- профили пользователей;
- данные пользователей;
- SQL-сервер с базой данных;

(2) backup сервер Shark включает сервисы:

- backup данные компьютеров домена;
- информационно–правовые системы: Консультант +, Гарант;
- Private FTP сервер;

(3) терминальный сервер, обслуживающий работу компьютерных классов;

(4) сервер системы видеонаблюдения;

(5) 1С сервер, обслуживающий работу бухгалтерии:

- база данных 1С;
- конфиденциальные документы бухгалтерии;

Кроме того, рабочие станции персонала содержат конфиденциальные данные и различную ценную информацию по образовательному процессу, потеря которой недопустима. Немаловажна работа компьютерной техники в целом, так как выход из строя одних компонент системы может нарушить весь образовательный процесс.

Как и в любой информационной системе, в данной ИС имеются объекты типа пользователь. В ИС Университета существует три вида объектов этого типа: администраторы, сотрудники Университета, студенты. Для каждого вида существуют свои привилегии и права доступа, а так же множество других настроек.

2.2. Методы анализа уязвимых элементов ИС

Для того, чтобы будущая система информационной безопасности компьютерной сети была эффективна, был проведен тщательный анализ уязвимых элементов ИС. Качественный анализ подразумевает всестороннее исследование уязвимостей ИС, в том числе с помощью различного программного обеспечения.

Анализ уязвимых элементов ИС может быть достаточно эффективен, если его проводить как с позиции администратора системы, так и с позиции потенциального злоумышленника. Стандартная методика [2] обнаружения/сканирования доступа корпоративной сети состоит в следующем:

(1) определение маршрутов доступа в сеть;
(2) запрос DNS[2];
(3) идентификация хостов;
(4) сканирование сетевых служб;
(5) сканирование на предмет уязвимых мест.

Кроме того, необходимо проверять уязвимости служб таких как: FTP, NetBIOS, DNS, DHCP.

Данные стандартные методы использовались на этапе аудита информационной безопасности Университета, кроме того, было использовано самое современное программное обеспечение для обнаружения уязвимостей.

После проведения сравнительного анализа программных средств для сканирования уязвимостей с использованием статей и практических тестов, в том числе использовались материалы учебного центра

[2]Доменная служба имен — ru.wikipedia.org/wiki/DNS

«Информзащита»[3], был выбран наиболее подходящий сетевой сканер безопасности по следующим параметрам:

(1) наличие бесплатной демонстрационной версии программы;
(2) наилучшие показатели по поиску уязвимостей;
(3) наименьшее число ошибок из всех представленных сканеров;
(4) удобство работы и простота интерфейса.

Сетевым сканером безопасности, удовлетворяющим всем этим параметрам, стал программный продукт XSpider[4] от компании Positive Technologies. Данное программное обеспечение обладает множеством возможностей, являющихся базовыми для обеспечения самого высокого качества и надежности в поиске уязвимостей.

Таким образом, во время проведения аудита информационной безопасности компьютерной сети Университета, были использованы не только опыт и знания по администрированию компьютерных сетей, но и стандартные методы анализа уязвимостей, а так же специальные современные программные средства. Все это позволило добиться хороших результатов на этапе аудита информационной безопасности и выявить множество проблем и нарушений.

2.3. Результаты аудита информационной безопасности компьютерной техники Университета

В ходе выполнения аудита информационной безопасности компьютерной сети Университета были обследованы все рабочие станции и серверы с целью выявления нарушений в области информационной безопасности. Данная проверка показала, что в организации имеются нарушения и уязвимости, которые могут привести к потерям информации и срыву образовательного процесса. Данные уязвимости требуют тщательного анализа и скорейшего устранения. По завершении проверки была составлена докладная записка на имя руководителя Группы компьютерной поддержки с перечнем всех нарушений.

На следующем шаге работы были проанализированы все уязвимости и связанные с ними риски. Были составлены материалы, демонстрирующие вероятности реализации угроз вызванных наличием уязвимостей. Каждой уязвимости была сопоставлена угроза потери

[3]Сравнительный анализ сканеров безопасности Учебного центра «Информзащита» — http://www.ptsecurity.ru/compare2.asp

[4]XSpider — http://www.ptsecurity.ru/xs7.asp

информации или несанкционированного доступа в систему и вероятность реализации злоумышленниками данной угрозы.

Итогами первой стадии разработки системы стали официальные документы, представленные руководству и наглядно отражающие реальную ситуацию в области информационной безопасности компьютерной сети «Университета города Переславля» им. А. К. Айламазяна.

3. Вторая стадия — направления и способы защиты

На втором этапе разработки системы безопасности было принято решение об устранении всех уязвимостей, выявленных на этапе аудита. Кроме того, были определены защищаемые ресурсы, располагающиеся на серверах и рабочих станциях персонала. В качестве базовой операционной системы, на основе и под управлением которой будет строиться система информационной безопасности, была выбрана Microsoft Windows Server 2003 R2[5]. Данная ОС является наиболее подходящей для развертывания групповых политик и политик аудита безопасности. Немаловажным при выборе платформы для системы стало то, что в организации уже имелась неплохая серверная база под управлением данной ОС с выделенным доменным контроллером и каталогом Active Directory[6]. Совместно с представителями Группы компьютерной поддержки Университета были выбраны основные направления построения системы безопасности. Ими стали:

(1) серверные технологии (Active Directory, Group Policy, Audit Policy);
(2) протоколы аутентификации и передачи данных (LM, NTLM, NTLMv2, Kerberos, IPSec)[7];
(3) шифрование данных;
(4) ограничение прав пользователей и доступа к объектам;
(5) мониторинг рабочих станций и серверов;
(6) шаблоны безопасности.

---

[5]Microsoft Windows Server 2003 — www.microsoft.com/rus/WindowsServer2003

[6]Служба каталогов — http://ru.wikipedia.org/wiki/Active_Directory

[7]Информация по существующим протоколам аутентификации в ОС семейства Windows — http://www.osp.ru/win2000/2005/05/177754/_p2.html

4. Третья стадия — реализация защиты

На третьем этапе разработки системы информационной безопасности были реализованы конкретные методы по направлениям построения системы, выбранные на второй стадии проекта.

За основу системы информационной безопасности компьютерной сети Университета был взят доменный контроллер Shark2 под управлением Windows Server 2003 R2. На базе данного доменного контроллера реализуются групповые политики, распространяющиеся на все рабочие станции и серверы домена и политики аудита безопасности. Групповые политики представляют собой множество различных настроек компьютеров и учетных записей пользователей, в том числе настроек, обеспечивающих безопасность домена и ограничение прав пользователей. Кроме того, групповые политики позволяют настроить и обеспечить выполнение единой политики аудита безопасности, направленной на предупреждение и выявление инцидентов нарушения безопасности.

Групповая политика является очень эффективным средством, так как позволяет администратору создавать стандартную конфигурацию компьютера сети. Объекты групповой политики (GPO) представляют собой значительную часть решения для управления параметрами, подходящего для любой организации, так как позволяют администраторам вносить изменения в параметры безопасности одновременно на всех компьютерах в домене или подразделах домена. С помощью групповых политик на этапе разработки системы информационной безопасности были применены следующие типы изменений параметров безопасности:

- изменение разрешений для файловой системы;
- изменение разрешений для объектов реестра;
- изменение параметров в реестре;
- изменение назначений прав пользователя;
- настройка системных служб;
- настройка журналов аудита и событий;
- установка политик паролей и учетных записей. [8]

В качестве протоколов аутентификации доменных компьютеров были выбраны — Kerberos и NTLMv2. Данные протоколы являются

[8] Рекомендации по политикам безопасности для Windows Server 2003 — http://www.microsoft.com/rus/technet/security/default.mspx

наиболее безопасными и защищенными, т.к. из 20 существующих инструментов взлома пароля только два работают с NTLMv2 и лишь один — с Kerberos. Предприняв несколько простых шагов, исключаем и эти 3 угрозы. Для предотвращения попыток разгадывания и сброса пароля были приняты следующие меры:

(1) отключено хранение LM–хешей;
(2) отключены все протоколы аутентификации, кроме NTLMv2 и Kerberos;
(3) запрещена начальная загрузка со сменных носителей;
(4) активизирована блокировка учетной записи после неверного ввода пароля.

Следующим направлением в защите информации является шифрование данных. В качестве системы шифрования данных была выбрана встроенная в Windows Encrypted File System. Данная система шифрования отличается простотой, надежностью и быстротой работы, а кроме того, для шифрования данных не требует развертывания каких либо дополнительных систем. Для шифрования файла используется случайно сгенерированный 128-битовый ключ DES (в международных версиях Windows 2000 используются 40-битовые ключи). Этот ключ шифруется на открытом асимметричном ключе пользователя и в таком виде сохраняется в новом атрибуте файла под названием «поле шифрования данных». При создании «поля восстановления данных» файла используется открытый ключ агента восстановления. Когда пользователь пытается открыть файл, для расшифрования поля шифрования данных он применяет свой секретный асимметричный ключ, а затем для расшифрования самого файла использует извлеченный в результате этой операции ключ шифрования файла.

5. Заключение

Результатом данной работы стало значительное улучшение уровня информационной безопасности компьютерной сети «Университета города Переславля» им. А. К. Айламазяна. Во время разработки системы было выявлено и устранено множество угроз безопасности, внедрены серверные решения в области групповых политик и политик аудита, обеспечена работа компьютеров по более надежным протоколам аутентификации. Кроме того было реализовано множество других решений по направлениям:

(1) ограничение прав пользователей и доступа к объектам;
(2) мониторинг рабочих станций и серверов;
(3) шаблоны безопасности;
(4) управление рабочими станциями;
(5) создание резервных копий данных.

Список литературы

[1] Белов Е. Б. Основы информационной безопасности. — М.: Горячая линия – Телеком, 2006. — 544 с.

[2] Домарев В. В. Безопасность информационных технологий. Методология создания систем защиты. — К.: Диасофт, 2002. — 688 с.

[3] Домарев В. В. Защита информации и безопасность компьютерных систем. — К.: Диасофт, 1999. — 480 с.

A. S. Shalaurov. *Developing security system of computer network "University of Pereslavl named after A.K. Aylamazyan"* // Proceedings of Progranm Systems institute scientific-practical conference "Program systems: Theory and applications", devoted to the 15^{th} anniversary of Pereslavl University named A. K. Ailamazyan. — Pereslavl-Zalesskij, 2008. — p. 253 — 264. — ISBN 978-5-901795-13-2 *(in Russian).*

Abstract. This work describes developing security system of computer network "University of Pereslavl named after A.K. Aylamazyan". Developing security system is necessary because information security is critical and very important for business today. This system is developed for protection of different information objects and all computer network.

Перевод проверен: Н. А. Прохорова