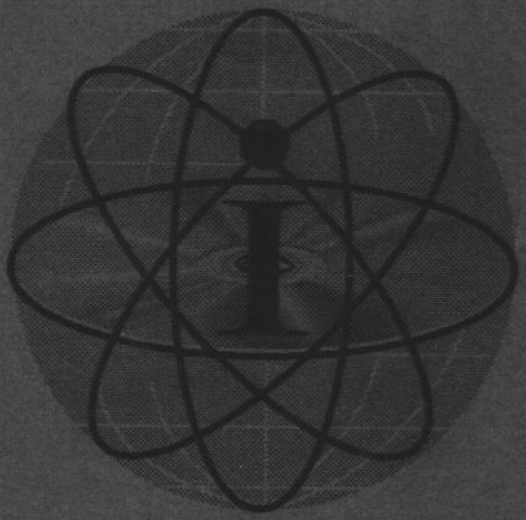
ПРИКЛАДНЫЕ ИНФОРМАЦИОННЫЕ ТЕХНОЛОГИИ



В НАУКЕ, ТЕХНИКЕ, ЭКОНОМИКЕ

МАТЕРИАЛЫ НАУЧНОЙ СЕССИИ

г. Волгоград, 24—25 апреля 2003 г.

МИНИСТЕРСТВО ОБРАЗОВАНИЯ
РОССИЙСКОЙ ФЕДЕРАЦИИ
ВОЛГОГРАДСКИЙ ГОСУДАРСТВЕННЫЙ УНИВЕРСИТЕТ

ПРИКЛАДНЫЕ ИНФОРМАЦИОННЫЕ ТЕХНОЛОГИИ В НАУКЕ, ТЕХНИКЕ, ЭКОНОМИКЕ

Материалы Научной сессии
г. Волгоград, 24—25 апреля 2003 г.

Волгоград 2003

ББК 72я431
П75

Прикладные информационные технологии в науке,
П75 технике, экономике: Материалы Научной сессии, г. Волгоград, 24—25 апреля 2003 г. — Волгоград: Изд-во ВолГУ, 2003. — 116 с.

ISBN 5-85534-745-1

Сборник включает статьи профессорско-преподавательского состава, студентов и аспирантов, отражающие основные положения их докладов на Научной сессии, проходившей в ВолГУ 24—25 апреля 2003 года.

ISBN 5-85534-745-1

[4] Поппель Г., Голдстайн Б. Информационные технологии — миллионные прибыли. М., 1990. С. 81—82.

[5] Мелюхин И.С. Информационное общество: истоки, проблемы и тенденции развития. М., 1999. С. 88.

[6] Эванс Ф. Указ. соч. С. 106.

В.В. Полубояров
аспирант, ассистент

ОБЕСПЕЧЕНИЕ БЕЗОПАСНОСТИ ИНФОРМАЦИОННОЙ СИСТЕМЫ «ЗДОРОВЬЕ НАСЕЛЕНИЯ»

Разрабатываемая авторами информационная система (ИС) «Здоровье населения» содержит в числе прочих персональные данные. Персональные данные на основании ст. 11 Федерального закона РФ «Об информации, информатизации и защите информации» № 24 от 25.03.95 относятся к конфиденциальной информации и подлежат защите. Необходимость построения защищенной ИС также обусловлена тем, что в качестве среды передачи в ней используется сеть Internet, и соответственно, ИС является потенциально уязвимой.

Цель работы — разработка стратегии обеспечения безопасности информационной системы «Здоровье населения», реализованной на платформе Windows 2000 Server. Задача состоит в анализе рисков, связанных с использованием сетей общего доступа для связи между компонентами информационной системы, разработке модели, обеспечивающей требуемый уровень безопасности, и определении шагов, требуемых для реализации выбранной модели безопасности.

Представленная модель безопасности основана на стратегии Microsoft Operations Framework[1]. Согласно этой стратегии, шаги, требуемые для создания и поддержания защищенной среды для информационной системы на серверах под управлением Windows 2000, состоят в разработке и реализации:

1) политики безопасности;
2) эшелонированной стратегии безопасности;
3) изоляции сервера;
4) антивирусной стратегии;

5) стратегии резервного копирования и восстановления;
6) стратегии управления патчами;
7) стратегий аудита и обнаружения вторжений;
8) плана реакции на инциденты.

Исходя из положений инициативы Strategic Technology Protection Program (STPP)[2], процесс обеспечения безопасной среды состоит из двух связанных фаз: создания безопасной среды (Get Secure — процесс достижения приемлемого уровня безопасности) и сохранения безопасности среды (Stay Secure — поддержание безопасности среды, осуществление превентивных действий против возникающих угроз, а также эффективная реакция на возникающие инциденты).

Первым этапом при построении системы безопасности ИС «Здоровья населения» является определение рисков. Под риском понимается результат анализа угроз в приложении к защищаемой среде[3]. Качественное определение рисков предполагает построение классификации угроз, уязвимостей, возможностей использования уязвимостей и контрмер в контексте информационных технологий — безопасности ИС «Здоровье населения». Для количественной оценки рисков необходимо определить существующие риски, их приемлемый уровень и поддерживать риски на этом уровне или ниже. Риск уменьшается посредством увеличения уровня безопасности. В работе приводится только качественный анализ рисков. Ключевыми при управлении рисками являются следующие понятия: ресурс, угроза, уязвимость, контрмера и возможность эксплуатации уязвимости[4].

Ресурсы являются объектом защиты в среде ИС. Они включают в себя данные, приложения, серверы, маршрутизаторы и персонал (см. рис. 1).

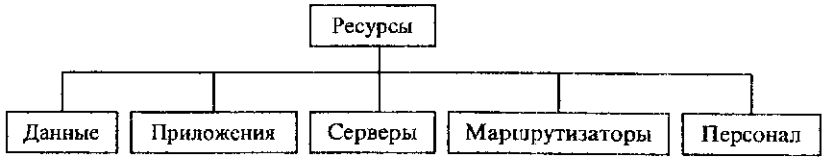


Рис. 1. Категории ресурсов

Под угрозой понимается человек, место или предмет, который имеет потенциальный доступ к ресурсам и может нанести им ущерб[5]. При построении модели безопасности будем учитывать угрозы физические (например, сбой напряжения питания), непреднамеренные (например, неинформированные сотрудники и клиенты), преднамеренные (например, атакующие) (см. рис. 2).

Рис. 2. Категории угроз

Под уязвимостью подразумевается место, в котором ресурс чувствителен к атаке[6]. Будем рассматривать уязвимости, причинами которых является программное и аппаратное обеспечение (например, устаревшее антивирусное программное обеспечение), коммуникации (например, протоколы, не поддерживающие шифрование) и человеческий фактор (например, небезопасные информационно-справочные процедуры) (см. рис. 3).

Рис. 3. Рассматриваемые причины уязвимостей

Под возможностью эксплуатации уязвимости понимается наличие способа использования уязвимости ресурсов. Рассматриваемые при построении модели безопасности ИС «Здоровье населения» возможности эксплуатации уязвимостей представлены на рис. 4. Их результатом может стать потеря конфиденциальности (например, несанкционированный доступ), потеря целостности данных (например, дезинформация), а также недоступность данных (например, отказ в обслуживании).

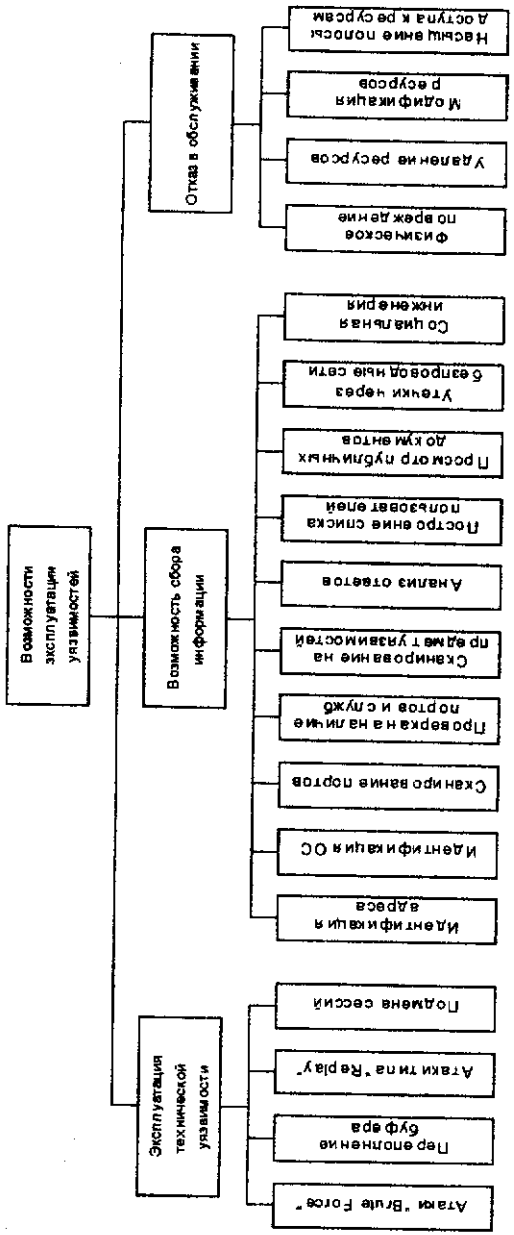


Рис. 4. Возможности эксплуатации уязвимостей

Контрмеры, предусмотренные моделью безопасности, применяются для противодействия угрозам и уязвимостям[7]. Для снижения риска ИС «Здоровье населения» используется стратегия многоуровневой защиты (см. рис. 5). Разработанная на ее основе архитектура системы безопасности представлена на рис. 6.

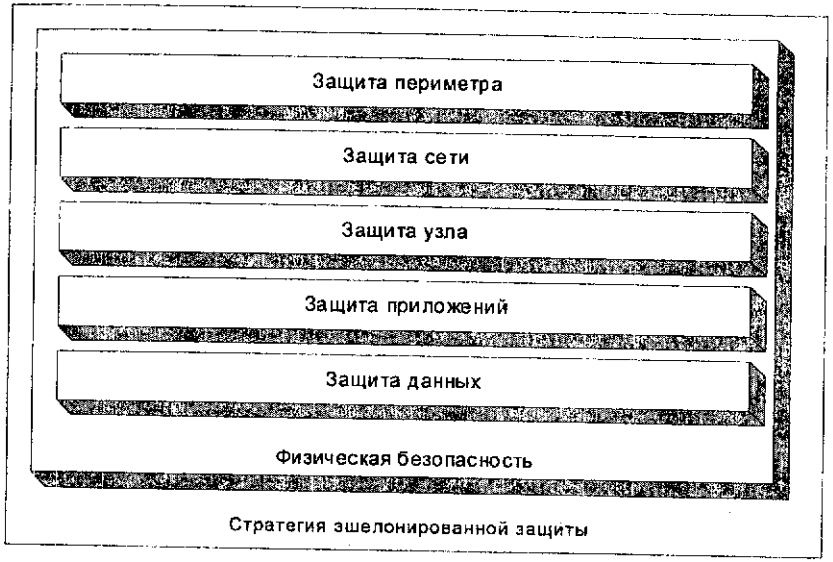


Рис. 5. Стратегия многоуровневой защиты ИС «Здоровье населения»

При построении системы безопасности ИС «Здоровье населения» для обеспечения физической безопасности осуществлена изоляция серверов и коммуникационных элементов от посторонних в выделенном помещении. Для обеспечения бесперебойного электропитания применяются решения компании APC. Защита периметра состоит в фильтрации нежелательного трафика (предварительная фильтрация на пограничном маршрутизаторе Catalyst 2600 и окончательная на межсетевом экране PIX 506). Для защиты сети применяется аутентификация и авторизация пользователей с использованием AAA-службы TACACS+ и технологии Remote VPN (шлюз — PIX 506, клиент — Cisco Secure VPN Client, аутентификация — по протоколу RSA, трафик шифруется по алгоритму DES, используются 128-битные функции MD5)[8]. Обеспечение безопасности сервера производится на основе его роли.

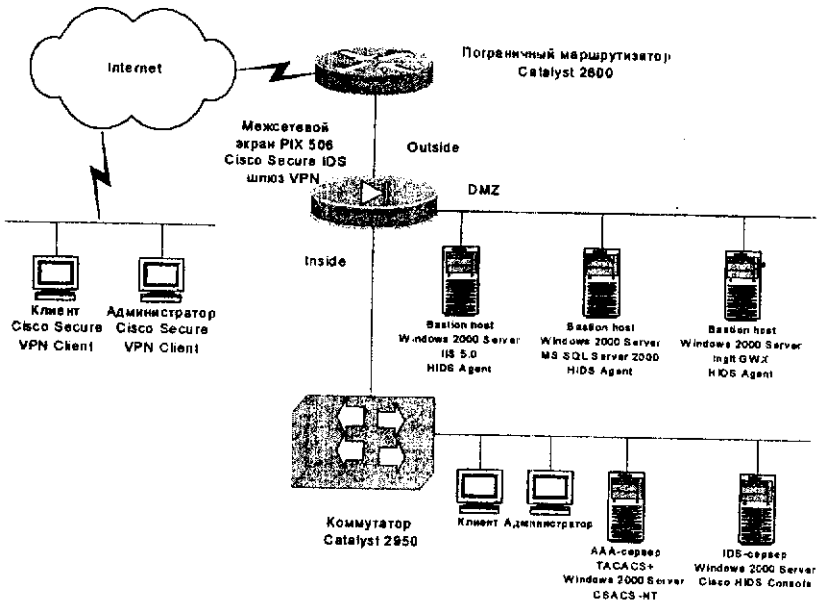


Рис. 6. Архитектура защищенной ИС

В рассматриваемой ИС присутствуют HTTP-сервер (IIS 5.0), сервер БД (MS SQL 2000) и ГИС-сервер (Windows 2000 Server + Ingit GWX). Важным компонентом модели безопасности является аудит безопасности среды и системы обнаружения вторжений (Intrusion Detection Systems — IDS). Для анализа сигнатур в пакетах прикладного уровня и реализации соответствующих политик аудита применяется встроенный в PIX 506 алгоритм Cisco Secure IDS. Мониторинг узлов осуществляется посредством использования пакета Cisco Host IDS 2.5. Антивирусная стратегия на клиентских и администраторских местах реализована при помощи пакета DrWeb 4.29. Безопасность данных обеспечивается файловой системой с шифрованием EFS. Резервное копирование осуществляется на регулярной основе, используются CD-RW-диски.

Разработанная модель безопасности является модульной, что позволяет при необходимости заменять и добавлять отдельные компоненты. Многоуровневая архитектура позволила создать комплексную систему безопасности, защищающую как от внешних, так и от внутренних угроз. В настоящее время проводится покомпонентная реализация представленной системы безопасности на основе разработанной модели. В работе не рассмотрены вопросы тестирования защищенности ИС.

Примечания

[1] Microsoft Prescriptive Guidance. Security Operations Guide on Windows 2000 Server. Microsoft Corporation, 2002.

[2] Microsoft Strategic Technology Protection Program Website // http://microsoft.com/security/msttp.asp.

[3] ISO/IEC Common Criteria for Information Technology Security Evaluation. V. 2.1. August 1999.

[4] Microsoft Prescriptive Guidance...

[5] Ibid.

[6] Ibid.

[7] Microsoft Prescriptive Guidance...; ISO/IEC...

[8] Chapman Jr.D., Fox A. Cisco Secure PIX Firewalls. Cisco Press, 2002.

Д.В. Марусин
аспирант, ассистент

ПРОЕКТИРОВАНИЕ ПОДСИСТЕМЫ РАЗГРАНИЧЕНИЯ ДОСТУПА ДЛЯ WEB-ОРИЕНТИРОВАННОЙ ИНФОРМАЦИОННОЙ СИСТЕМЫ

В настоящее время одним из требований, предъявляемых к информационным системам, работающим в глобальной вычислительной среде, является наличие подсистемы разграничения доступа. Для систем, содержащих информацию конфиденциального и служебного характера, наличие таких подсистем является обязательным. Существует большое количество подходов к обеспечению безопасной работы информационных систем в среде Интернет:

- использование механизмов защиты протокола IP (IP security);
- использование межсетевых экранов и средств разделения трафика;