

**Совместное рабочая сессия ЕЭК/Евростата по
Конфиденциальности статистических данных**
(Скопье, Бывшая республика Югославии Македония
14-16 марта 2001 года)

Рабочий документ no. 36

Тема IV: Прогресс в исполнении методов и техники исполнения СДС в центральной и восточной Европе

**ВЛИЯНИЕ РАЗВИТИЯ ТЕХНОЛОГИЙ ПРОГРАММИРОВАНИЯ, КОММУНИКАЦИЙ И
ВЫЧИСЛИТЕЛЬНОЙ ТЕХНИКИ НА УПРАВЛЕНИЕ ДОСТУПОМ К
СТАТИСТИЧЕСКИМ ДАННЫМ**

Вспомогательный доклад

Документ представлен Агентством по статистике Республики Казахстана ¹

1. Для сбора статистической информации из регионов Агентство РК по статистике использует свою корпоративную сеть передачи данных, основанную на сети «Банкнет» Центра межбанковских и финансовых телекоммуникаций (ЦМФТ). Корпоративная сеть органов статистики Казахстана включает в себя:

- Локальную вычислительную сеть республиканского уровня;
- Локальные компьютерные сети областных управлений по статистике;
- Компьютеры отдельных абонентов районного уровня .

2. Локальная вычислительная сеть (ЛВС) республиканского уровня взаимодействует с локальными компьютерными сетями областных управлений по наземным выделенным телекоммуникационным каналам. Компьютеры отдельных абонентов районного уровня соединяются средствами коммутируемой модемной связи с областной ЛВС. Такая сеть позволяет оперативно осуществлять сбор и передавать информацию из районов в областные управления, откуда проверенная интегрированная информация отправляется в центр (г. Алматы). Для обеспечения ввода данных на районном уровне разработаны специальные приложения по вводу, контролю, создана подсистема районного уровня, осуществляющая первоначальный сбор данных. Реализовано ее подключение к системе по обработке данных статистических исследований, функционирующей на областном и республиканском уровнях.

3. Кроме того, созданы возможности обмена информацией любого типа с использованием выхода во внешние глобальные телекоммуникационные и информационные системы. Проводятся работы по обеспечению предоставления информации заинтересованным организациям и клиентам из любого территориального узла корпоративной сети. Планируется осуществить взаимодействие статистической информационной системы с внешними поставщиками информации и пользователями, с информационными системами центральных экономических органов, отраслевыми и региональными системами управления и крупными предприятиями. Будут внедрены технологии получения информации в электронном виде непосредственно от крупных предприятий.

¹ Автор: Алионора Косьяненко

Основные методы защиты сети

4. Поддержание массовых и разнообразных связей органов статистики с внешним миром с одновременным обеспечением безопасности этих коммуникаций является сегодня главной задачей и предполагает постоянное развитие средств защиты статистических данных. Для защиты данных в intranet применяются защищенные Web-серверы, внутренние и внешние брандмауэры, планируется использование smart-карточек, систем шифрования. Перспективные средства защиты данных предприятия должны учитывать появление новых технологий и сервисов, а также удовлетворять общим требованиям, предъявляемым сегодня к любым элементам корпоративной сети. Средства защиты должны основываться на открытых стандартах.

5. Одним из главных условий при построении защиты сети является использование интегрированных решений- интеграция различных технологий безопасности между собой для обеспечения комплексной защиты информационных ресурсов статистики - например, интеграция межсетевых экранов (firewall) с VPN-шлюзом (Virtual Private Network) и транслятором IP-адресов, интеграция средств защиты с остальными элементами сети - операционными системами, маршрутизаторами, службами каталогов и т.п. Система защиты должна обеспечивать эффективную работу многочисленных территориальных подразделений статистики, предприятий-поставщиков информации, множество потенциальных клиентов. Вовлечение в автоматизированную обработку информации практически всех подразделений статистики и повышение требований к защите обрабатываемой и передаваемой информации приводит к необходимости использования межсетевых шлюзов с установленным дополнительным программным обеспечением firewall и между внутренними подсетями. Существует несколько вариантов построения защиты от попыток взлома корпоративного Web-узла с использованием программно-аппаратных "защитных стен" (Firewall). Одна из возможных конфигураций когда Web-сервер приложений Oracle располагается между двумя Firewall - внутренним и внешним. Внешний Firewall защищает Web-сервер приложений от прямых атак из открытой интернет-сети. Он же реализует механизм шифрования запросов, передаваемых Web-сервером приложений во внешнюю сеть. Внутренний Firewall выполняет дополнительную защиту участка между Web-сервером и сервером базы данных и может также выполнять дополнительное шифрование SQL запросов на этом участке сети.

6. Firewall должна осуществлять ряд полезных функций по контролю соединений HTTP и FTP: запрещение доступа к спискам URL, вырезание тегов Java и ActiveX из загружаемых страничек, антивирусная проверка файлов, ограничение доступа по паролю и т. п. При построении системы защиты важен выбор структуры сети. Сегментирование системы - это один из возможных методов реализации безопасности. Если информация предназначена только для группы специалистов, то лучше разместить ее на закрытом Web-сервере, а не в корпоративной intranet. Правильный выбор структуры сети обычно облегчает разработку политики безопасности и управления firewall и повышает устойчивость защиты. Во многих случаях неудачное размещение какого-либо сетевого объекта может создать трудности при контроле некоторых видов трафика и детектировании попыток взлома сети. Одним из примеров решения по выбору структуры сети является размещение общедоступных серверов - Web, FTP, SMTP, DNS в распределенной демилитаризованной зоне. С одной стороны, эти серверы должны быть доступны для всего внешнего мира, с другой - необходимо строго контролировать попытки доступа к ним. Предпочтительным вариантом является подключение каждого из открытых серверов на отдельный сетевой интерфейс firewall. Это дает возможность со стопроцентной уверенностью контролировать весь трафик такого сервера и гарантирует защиту одного открытого сервера от другого в случае нарушения безопасности одного из них.

Дополнительные защитные меры

7. Существующие развитые механизмы безопасности, такие как сетевое кодирование и сложные схемы идентификации надежно защищают данные, но кроме того нужны некоторые

дополнительные меры организационного характера для того, чтобы обеспечить безопасность производственной среды. Перечислим некоторые из них:

- Необходимо регулярно тестировать брандмауэры для проверки их неустойчивости, применяя специальное программное обеспечение.
- Следует исключить ошибки операторов информационных систем. Результатом такой ошибки может стать брешь в системе защиты, потеря данных, останов или выход из строя системы. Один из путей минимизации рисков, связанных с этим типом угроз, — максимальная автоматизация статистического производственного процесса, контроль за точным соблюдением инструкций и повышение квалификации персонала.
- Организация надежного хранения резервных копий. Выдача из библиотеки ленты с резервной копией и возможность доступа к ее данным должны строго контролироваться. Необходимо организовать санкционирование запросов лент, а также регистрацию момента извлечения и возвращения ленты. Если для получения резервной копии данные копируются с одного диска на другой (дискковое резервное копирование), то диск с копией базы данных необходимо поместить в недоступное для несанкционированного чтения место.
- Разработчики в большинстве случаев слабо контролируют свою среду разработки и проводят тестирование на полной копии производственной базы данных. При этом любой внутренний служащий или внешний консультант могут получить полный доступ к наиболее важным активным данным. Во время тестирования приложения количество пользователей, имеющих доступ к рассекреченным данным, как правило, возрастает. Для улучшения защиты производственной базы данных можно изолировать ее от среды разработки. Для этого необходимо отменить доступ разработчиков к производственному серверу на уровне операционной системы и обеспечить стандартный контроль за выполнением изменений и не разглашать имя базы данных и сервера, выполняющих производственные приложения. Возможно следует вообще запретить использование производственной базы данных для разработки и тестирования.
- Пользователям следует изменять их пароли с частотой, соответствующей общей политике безопасности. Можно уменьшить срок действия пароля и, тем самым, предотвратить использование устаревших паролей.

Организация безопасности корпоративной информационной системы на основе использования средств фирмы Oracle

8. В настоящее время в ИВЦ Агенства РК по статистике разрабатывается информационная подсистема безопасности с применением программных продуктов фирмы Oracle. Проблемы безопасности корпоративной информационной системы будут решаться с использованием двух компонентов системы: администрированием сервера БД Oracle8 и сервера приложений Oracle.

9. Для защиты сервера Oracle используется сертифицированная цифровая аутентификация. Когда при входе в корпоративную сеть пользователь вводит имя и пароль, то они сразу же шифруются и в зашифрованном виде передаются по открытым каналам связи на сервер приложений. Используется также эффективный механизм защиты - электронная подпись, исключающий ситуацию умышленного использования третьим лицом чужого открытого ключа, он применяется для дополнительной проверки данных доступных через открытые сети. Существует также метод аутентификация базы данных, который позволяет хранить имена и пароли не в файлах операционной системы, а в базе данных. Это означает, что администратору приходится управлять одним набором имен пользователей и паролей для доступа как к Web-серверу, так и к базе данных. Применение этого метода повышает степень защиты данных, так как сервер данных обеспечивает более детализированное управление доступом, чем операционная система. Использование СУБД Oracle, позволяет производить шифрование передаваемых данных, программного кода и хранимых процедур для каждой сессии передачи данных между сервером приложений и сервером БД. Даже если информационный пакет проходит по сети с различными протоколами, он все равно остается

зашифрованным на всех ее участках. Помимо шифрования основным ключом при этом используются методы шифрования контрольных сумм для обеспечения целостности передаваемых данных.

10. Подсистема защиты информации предназначена для компенсации угроз информационной безопасности системы, осуществляемых традиционными средствами сетевого доступа, а также компенсации угроз со стороны технического (эксплуатирующего) персонала, зарегистрированных пользователей и внешних абонентов путем внешнего мониторинга состояния системы, контроля и анализа действий операторов и удаленного централизованного управления средствами защиты информации, входящими в состав подсистемы.

11. Проектирование системы информационной безопасности начнется с разработки следующих документов:

- “Исходные данные по структуре системы (исследование угроз информационной безопасности сетевого уровня)”;
- “Концепция информационной безопасности системы на сетевом уровне”. При сборе, анализе и подготовке исходных данных по структуре системы должны быть проанализированы с точки зрения информационной безопасности:
 - Компоненты и топология сети;
 - Состав коммуникационного оборудования;
 - Характеристики каналов связи;
 - Коммуникационные протоколы и необходимые сервисы, их локализация в корпоративной сети, "точки" и маршруты доступа;
 - Классификация критичных ресурсов сети (адресная информация, служебная информация, информация в центрах хранения и обработки данных, трафик в каждом из каналов его распространения, системное программное обеспечение и средства администрирования, прикладное программное обеспечение и т.д.);
 - Обзор, описание и классификация атак на информационные ресурсы сети;
 - Обзор, описание и сравнительный анализ систем для обеспечения информационной безопасности сетевого уровня.

12. В “Концепции информационной безопасности системы на сетевом уровне” определяются:

- Объект защиты и модель защищаемого объекта;
- Модели атакующей стороны (определение угрозы, атаки, атакующей стороны);
- Классификация потенциальных атакующих сторон. При разработке Концепции должны быть проведены следующие работы:
 - проведен анализ угроз информационной безопасности сетевого уровня;
 - приведены критерии оценки угроз информационной безопасности;
 - разработаны спецификации атак на объект защиты;
 - оценены критичности атак на объект защиты;
 - проанализированы критичность атак и приоритетность компенсации угроз информационной безопасности сети;
 - разработаны методы компенсации угроз информационной безопасности сетевого уровня;
 - определены принципы построения и основные функции системы защиты информации сетевого уровня;
 - разработаны методы компенсации угроз информационной безопасности;
 - определена этапность развертывания системы защиты.

13. Подсистема защиты информации сетевого уровня должна обеспечивать:

- ведение базы данных (БД) и обеспечение подотчетности действий технического персонала, эксплуатирующего оборудование системы;

- ведение БД внешних зарегистрированных абонентов системы и мониторинг доступа к информационным ресурсам абонентов системы из внешних сетей;
- сбор данных со специализированных устройств защиты информации (фильтрующие маршрутизаторы, межсетевые экраны, технические средства защиты графика и проч.);
- анализ целостности выделенных информационных ресурсов системы;
- накопление, систематизированное хранение, аудит регистрационных протоколов (журналов), формирование отчетов;
- защиту и компенсацию атак на критичные ресурсы системы, такие как: топология сети (адресная информация), служебная информация, график, информация в центрах обработки и хранения данных, системное программное обеспечение и средства администрирования, прикладное программное обеспечение;
- базирование на единой стандартизированной технологической основе и защиту сетевых объектов различного уровня сложности, от крупных сегментов локальных сетей до отдельных терминалов удаленных абонентов;
- совместимость с аппаратно-программными средствами и каналобразующим оборудованием системы и должна учитывать перспективы развития сети.

14. Внедрение новых средств защиты, в сочетании с аппаратными методами контроля сетевого трафика на различных участках корпоративной сети, даст возможность реализовать полноценную и надежную систему предупреждения несанкционированного доступа и утечки информации конфиденциального характера. При этом решаются многие проблемы, связанные с нарушением безопасности в сети и Интернет - обеспечивается неприкосновенность статистических данных и коммуникаций (с помощью шифрования и проверки целостности), проводится идентификация пользователей, баз данных и web-серверов (интегрированная поддержка идентификации), осуществляется безопасный удаленный доступ.