

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

## **ЗАЩИТА ИНФОРМАЦИИ ОТ НЕСАНКЦИОНИРОВАННОГО ДОСТУПА**

### **Вспомогательный доклад**

Документ представлен Госкомстатом Азербаджана<sup>1</sup>

1. Государственный Комитет Азербайджанской Республики по Статистике располагает огромным количеством статистической информации, характеризующей развитие почти всех областей деятельности страны. Вся информация в обязательном порядке поступает в адрес органов государственной статистики от респондентов, осуществляющих любой вид деятельности на территории республики, являясь конфиденциальной и должна быть закрыта от свободного доступа. Любой респондент в законодательном порядке располагает правом на сохранение тайны государственного, коммерческого, служебного и наконец личного характера. В этих целях в принятом в 1994 году Законе о Статистике Азербайджанской Республики специально была предусмотрена 11 статья “Статистическая тайна”, которая гласит: “Первичные статистические (индивидуальные) данные юридических и физических лиц являются конфиденциальными и представляют собой статистическую тайну. Любая умышленная или неосторожная передача органами государственной статистики сведений о юридических и физических лицах без их согласия государственным органам, предприятиям, организациям или гражданам, которые не имеют законного доступа к этим сведениям, или же публикация их в средствах массовой информации является разглашением сведений, составляющих статистическую тайну”. В результате утечки информации, как следствие, может быть нанесен моральный ущерб и самому Госкомстату, выражающийся в недоверии к нему со стороны респондентов и общественности. Это также может существенно повлиять на достоверность и полноту собираемой статистической информации и т. д. Во избежание вытекающих при разглашении статистической тайны последствий в органах государственной статистики предпринимаются надлежащие меры по защите информации от несанкционированного доступа. Так, согласно “Кодексу административных проступков”, утвержденному Милли Меджлисом в июле 2000 г., за разглашение статистической тайны к виновным лицам применяются следующие меры взысканий: физические лица штрафуются в размере от 15-ти до 25-ти минимальных окладов заработной платы, размер штрафа с должностных лиц составляет от 35-ти до 50-ти минимальных окладов заработной платы; одновременно за разглашение статистической тайны путем опубликования конфиденциальной информации в средствах массовой информации штраф с физических лиц взимается в размере от 30-ти до 40 минимальных окладов заработной платы, а с должностных лиц соответственно от 70-ти до 90.

---

<sup>1</sup> Авторы: Велиев А.М. и Аллахвердиев В.А.

2. Проблемы защиты информации от несанкционированного доступа особенно актуальны в современных вычислительных средах, представляющих собой сложные корпоративные сети Wide Area Network. Статистические организации большинства стран имеют территориально распределенную инфраструктуру и в силу этого они часто используют технологии WAN для сбора, обработки и распространения статистической информации. В этих системах широко используются технологии Intranet-Internet для передачи и распространения информации, технологии доступа в режиме on-line к базам данных, технологии сетевой обработки информации. Как правило, эти сети имеют развитые средства локального и удаленного доступа большого числа абонентов к ресурсам сети и, в частности, к базам данных. Естественно, что сохранность и конфиденциальность информации в таких системах является одной из первостепенных задач. Средства защиты информации устанавливаются с самого начала функционирования сети и развиваются параллельно с ее развитием.

3. В настоящее время в системе Госкомстата Азербайджана установлена и ускоренными темпами развивается корпоративная сеть. В течение 2001-го года эта сеть должна охватить всю систему Госкомстата, включая все ее территориально удаленные подразделения, расположенные в административных районах страны. Планируется обеспечение доступа к ресурсам этой сети в режиме on-line около восьмидесяти территориально удаленных подразделений Госкомстата. Кроме этого, услуги доступа к информации будут оказываться и сторонним заинтересованным организациям. Ближайшими задачами развития информационных технологий обработки статистических данных, которые планируется решать в среде WAN Госкомстата являются:

- автоматизация сбора первичных статистических данных путем применения WEB-технологий и E-mail;
- автоматизация передачи информации между удаленными и локальными клиентами внутри системы Госкомстата;
- применение сетевых технологий обработки статистической информации средствами промышленных распределенных баз данных;
- реализация современных методов распространения информации с помощью технологий WEB-сервиса.

4. Эти технологии предоставляют широкому кругу клиентов доступ к программным и информационным ресурсам сети и, следовательно, требуют применения надежных методов защиты информации от несанкционированного доступа.

5. Меры по защите информации всегда связаны с дополнительными затратами, порой значительными. Можно бесконечно усиливать меры по защите, затрачивая при этом все новые и новые средства. Здесь всегда надо руководствоваться принципом достаточности и теми реальными финансовыми возможностями, которыми мы располагаем. Тем более, что мы, как и все другие страны с переходной экономикой работаем в условиях острой нехватки средств.

6. Ниже приводим некоторые достаточно эффективные методы защиты информации, которые мы применяем в системе Госкомстата Азербайджана.

7. **Выбор сетевой операционной системы.** Любая сетевая операционная система имеет различные встроенные средства защиты сетевых ресурсов. Разница лишь в способах организации этой защиты и ее эффективности. В любом случае, выбирая сетевую операционную систему, следует проверить сертифицирована ли она по классу сетевой защиты уровня C2. Сетевая операционная система Novell NetWare 5, используемая у нас имеет богатый арсенал таких средств, основные из которых перечислены ниже:

- доступ к сети только по индивидуальному паролю. Информация о паролях пользователей закодирована и полностью защищена от проникновения;
- разграничение по уровню доступа. Сетевые ресурсы и приложения классифицируются по уровням и доступ к ним зависит от уровня пользователя;

- установка индивидуальных ограничений доступа. Администратор может установить любые ограничения доступа для любого пользователя или любого приложения;
- ограничения по времени доступа. Пользователь может работать только в период отведенного для него интервала времени;
- фиксирование рабочей станции. Данный пользователь может войти в сеть только из одной определенной для него рабочей станции;
- контроль повторного вхождения в сеть. Клиент не может войти в сеть повторно, если он в данный момент уже находится в сети;
- ограничение действий пользователя. Ограничиваются действия пользователя по какой-либо операции (например по операции записи);
- ограничения по доступу к приложениям. Пользователь может использовать только те приложения, к которым он имеет доступ.

8. Информация о правах пользователя хранится в его учетной информации, которая доступна только администратору. Действия администратора неограничены, но они регистрируются и могут быть проконтролированы независимым аудитором.

9. **Обучение обслуживающего персонала.** Во многом защищенность данных зависит от уровня подготовки обслуживающего персонала. Это умение оценивать ситуацию и применять в полной мере все встроенные в операционную систему средства защиты. Это относится в первую очередь к персоналу администраторов сети.

10. **Технические методы.** Сервер, активное сетевое оборудование и кабельная система должны быть максимально защищены от физического проникновения. Все серверное оборудование должно быть расположено в специальном помещении, защищенном от проникновения посторонних лиц. Активное сетевое оборудование должно быть размещено в специальных запирающихся шкафах. Незадействованные сетевые розетки в рабочих помещениях должны быть отключены от активного оборудования.

11. **Операционная система клиента.** Операционная система клиента должна надежно защищать информацию, хранящуюся на этой рабочей станции. Как показал опыт парольная защита Windows 95 легко удаляется и компьютер становится полностью доступным. Желательно всюду, где это возможно использовать систему Windows 2000 Workstation.

12. **Охранные мероприятия.** Все рабочие помещения офиса, где находится вычислительная техника должны быть под охраной в течении всего нерабочего времени. Желательно использование средств электронной охраны: датчиков движения, видеокамер и других охранных средств.

13. **Защита электронной почты.** Значительная часть информации в систему Госкомстата поступает и перемещается внутри посредством E-mail. Это в основном:

- первичная статистическая информация, направляемая отчитывающимися организациями органам статистики;
- информация, передаваемая между удаленными подразделениями Госкомстата;
- информация, передаваемая между локальными и удаленными клиентами;
- статистическая информация, передаваемая заинтересованным сторонним организациям.

14. Если электронная почта передается по сети Internet как обычное незакодированное письмо, то оно совершенно не защищено от чтения посторонними людьми. Дело в том, что копия такого письма остается как минимум на четырех компьютерах – у отправителя, на сервере провайдера отправителя, на сервере провайдера получателя и на компьютере получателя. Администраторы провайдеров имеют все программные средства перехвата, чтения и копирования этой почты. Отчитывающаяся в Госкомстат организация может даже и не подозревать, что отправляя свои отчеты, она сама разглашает свои данные. То же относится и к внутриведомственному обмену информацией через E-mail между удаленными

подразделениями Госкомстата. Для решения вопроса использования E-mail Госкомстат сам должен обеспечить безопасность этой технологии.

15. Решить проблему можно двумя путями:

- применением методов программного шифрования (например методом PGP-Pretty Good Privacy).
- установкой собственного Mail-сервиса, позволяющего организовать корпоративную почту в обход Internet. В этом случае клиент регистрируется в корпоративной сети Госкомстата, получает доступ к ней и вся его почта в обоих направлениях передается через Mail-сервер Госкомстата.

16. **Сетевая обработка данных.** Эффективная обработка статистической информации связана с применением промышленных реляционных СУБД, например Oracle. В среде этой СУБД разрабатываются приложения для групповой работы с базами данных, находящимися на сервере. Пользователи сети получают доступ к своей информации и участвуют в совместной работе с ними независимо от своего местонахождения. Защита в этом случае осуществляется путем разграничения администратором сети доступа к данным между приложениями. Сами приложения должны иметь защитные средства, ограничивающие доступ исполнителей работы как к информации, так и по кругу выполняемых операций. Необходимо иметь администратора баз данных, который бы выполнял необходимые защитные мероприятия по утечке информации из баз.

17. **Распространение информации.** Широкий доступ к информации осуществляется посредством доступа к данным через WWW-технологии. Однако в этом случае возможно несанкционированное проникновение к конфиденциальной информации баз данных. Обезопасить себя можно двумя способами:

- создать отдельную базу данных открытой распространяемой информации и только к ней организовать доступ из Web-страниц. Остальная информация должна быть недоступна для Internet.
- не пользоваться для хранения Web-страниц и информации сервером провайдера. Необходимо создать свой Web-сервер, который содержал бы распространяемые базы данных и не имел бы доступа к другим серверам сети, ответственным за хранение иной информации.

18. Системы безопасности сетей развиваются параллельно с самой сетью и требуют постоянного внимания и планирования. Во многом безопасность сети зависит от понимания важности этой проблемы руководством предприятия. Руководство должно своевременно решать вопросы финансирования мероприятий по безопасности, закупку необходимого оборудования, программных средств и обучение персонала. Экономия здесь может обернуться многократно большими финансовыми и моральными потерями в дальнейшем.