



**ЭКОНОМИЧЕСКИЙ
И СОЦИАЛЬНЫЙ СОВЕТ**

Distr.
GENERAL

CES/AC.71/2001/17 (Summary)
5 December 2000

RUSSIAN
Original: ENGLISH

**СТАТИСТИЧЕСКАЯ КОМИССИЯ и
ЕВРОПЕЙСКАЯ ЭКОНОМИЧЕСКАЯ КОМИССИЯ**

**КОМИССИЯ ЕВРОПЕЙСКИХ
СООБЩЕСТВ (ЕВРОСТАТ)**

КОНФЕРЕНЦИЯ ЕВРОПЕЙСКИХ СТАТИСТИКОВ

**Совместное совещание ЕЭК/Евростата по вопросам управления статистической
информационной технологией**
(Женева, Швейцария, 14-16 февраля 2001 года)

Тема (ii): Задачи и возможности статистических управлений, работающих в сетевой среде

**ПРОБЛЕМЫ, СВЯЗАННЫЕ С БЕЗОПАСНОСТЬЮ ПЕРЕДАЧИ ДАННЫХ
ЧЕРЕЗ СЕТИ, И СООТВЕТСТВУЮЩИЕ РЕШЕНИЯ, ВНЕДРЕННЫЕ
В ЦСУ ПОЛЬШИ**

Документ представлен Центральным статистическим управлением Польши¹.

СПЕЦИАЛЬНЫЙ ДОКУМЕНТ

РЕЗЮМЕ

1. Защита собираемой, обрабатываемой и распространяемой статистической информации является объектом пристального внимания каждого сотрудника Статистического управления. В то же время несомненно справедливым является утверждение о том, что невозможно обеспечить стопроцентную защиту во всех областях. На практике приходится мириться с определенным уровнем риска, поскольку по мере совершенствования систем защиты все более изощренными становятся и методы компьютерного взлома. Для эффективной защиты конфиденциальной информации необходимо определить возможные уязвимые компоненты, которые могут стать причиной нарушения конфиденциальности, целостности и содержания такой информации. В отношении каждого уязвимого компонента необходимо определить все реалистично возможные способы взлома защиты и разработать методы по предотвращению такого взлома. Порой

¹ Автор: Галина Агнешка Стегавска.

целесообразно поручать эту работу внешним специализированным компаниям, занимающимся эксплуатацией систем защиты данных.

2. Термин "политика защиты" охватывает все меры руководства, администрации, технического персонала, пользователей и всех других сотрудников организации по обеспечению необходимого уровня защиты статистической информационной системы. Данный уровень защиты определяется совокупностью используемых средств защиты. Их целью является регулирование доступа к ресурсам (оборудованию, программному обеспечению, документации, первичным данным), конфиденциальности данных, прав доступа и целостности данных.

3. Возможные проблемы, связанные со взломом защиты данных в компьютерных сетях, можно разбить на следующие три категории:

- ◆ умышленный взлом защиты - хищение ключа доступа или несанкционированное подключение к сети;
- ◆ несанкционированный доступ к данным - регистрация в системе с использованием похищенного или подобранного пароля;
- ◆ отказ в обслуживании - в результате взлома системы защиты пользователи не могут получить доступ к определенной услуге или всем услугам сети или сервера;

4. Основными методами, уже используемыми или планируемыми к использованию для защиты сетей, являются: идентификация (идентификация пользователей с помощью паролей), проверка прав доступа (проверка личности пользователя), санкционирование и контроль доступа (присвоение прав доступа пользователю), защита конфиденциальности информации, целостности данных, (обеспечение сохранности документов в ходе передачи) и цифровые подписи.

5. Еще одной проблемой является безопасный Интернет-доступ, а также доступ из Интернет к корпоративной локальной сети ЦСУ. Все ресурсы обработки данных Интранет ЦСУ защищены брандмауэром и, следовательно, недоступны внешним пользователям. Только WWW-серверы с базами данных общего доступа, не защищенные брандмауэром, открыты для доступа из Интернет. Пользователи, работающие в региональных статистических управлениях и локальной сети ЦСУ, имеют доступ к Интернет только через центральную систему брандмауэра. Использование услуг Интернет требует подтверждения прав пользователя и авторизации в случае таких услуг, как электронная почта, www, telnet и ftp. Система брандмауэра дополняется двумя маршрутизаторами, что еще более затрудняет попытки взлома системы.

6. Система защиты данных должна постоянно обновляться с использованием новых методов, обеспечивающих более высокий уровень защиты. С учетом этого ЦСУ в настоящее время ведет работу по следующим направлениям:

- ◆ определение слабых мест в используемой в настоящее время системе брандмауэра; в целях ее модификации или возможной замены;
- ◆ переход на операционные системы WINDOWS 2000 Servers и Windows 2000 PC;

- ◆ замена части оборудования, используемого в локальных сетях и корпоративной сети ЦСУ, оборудованием с более высоким уровнем защиты, например Switch L3, маршрутизаторами новых поколений;
- ◆ внедрение методов криптографии данных на сервере и различных уровнях территориально распределенной сети;
- ◆ обновление "Правил и норм для пользователей компьютерных сетей" и их внедрение.
