(1) More(больше) and more, the operations of our businesses(предприятий), governments(правительства), and financial institutions(учреждений) are controlled by information that exists only inside(которая существует только в) computer memories. Anyone(Каждый) clever enough(достаточно умный может) to modify this information for his own(для своих собственных) purposes(целей) can reap(снимать) substantial(хороший) re wards(урожай). Even worse(И что хуже), a number of people(целому ряду людей) who have done(которые совершили) this(это) and been caught(пойманы) at it have managed to get away without punishment(при этом удалось остаться без наказания).

(2) These facts have not been lost(не были упущены) on criminals(преступниками) or would-be criminals(или потенциальными преступниками). A recent Stanford Research Institute study of computer abuse was based on 160 case histories, which probably are just the proverbial tip of the iceberg(Последнее исследование Stanford'ского Научно-исследовательского Института злоумышленных действий на компьютере было основано на 160 случаях, которые вероятно являются только видимой частью айсберга.). After all(В конце концов), we only know about the unsuccessful(неудачных) crimes(преступлениях). How many(Сколько) successful(успешных) ones(те) have gone(которые остались) undetected(необнаруженными) is anybody's guess(никто не догадывается).

(3) Here are a few(несколько) areas(областей) in which(которых) computer criminals(преступления) have found the pickings all too easy(были обнаружены слишком легко).

(4) Banking(Банковское дело). All but the smallest banks now keep their accounts on computer files. Someone who knows how to change the numbers in the files can transfer(перемещать) funds at will. For instance, one programmer was caught having the computer transfer funds from other people's accounts to his wife's checking account. Often(Часто), tradition ally trained(традиционно обученные) auditors(ревизоры) don't know enough about the workings of computers to catch what is taking place right under their noses.

(5) Business(Бизнес). A company(компании) that uses(которые широко используют компьютеры) computers extensively(предлагают) offers many opportunities(много возможностей) to both dishonest(нечестным) employees(сотрудникам) and clever(умным) outsiders(посторонним). For instance(Например), a thief(вор) can have the computer ship the company's products to addresses of his own choosing. Or he can have it issue checks to him or his confederates for imaginary supplies or ser vices. People have been caught doing both.

(6) Credit Cards. There is a trend toward using cards similar to credit cards to gain access to funds through cash-dispensing terminals. Yet, in the past, organized crime has used stolen or counterfeit credit cards to finance its operations. Banks that offer after-hours or remote banking through cash-dispensing terminals may find themselves unwillingly subsidizing organized crime.

(7) Theft of Information. Much personal information about individuals is now stored in computer files. An unauthorized person with access to this information could use it for blackmail. Also, confidential information about a company's products or operations can be stolen and sold to unscrupulous competitors. (One attempt at the latter came to light when the competitor turned out to be scrupulous and turned in the people who were trying to sell him stolen information.)

(8) Software Theft. The software for a computer system is often more expensive than the hardware. Yet this expensive software is all too easy to copy. Crooked computer experts have devised a variety of tricks for getting these expensive programs printed out, punched on cards, recorded on tape, or otherwise delivered into their hands. This crime has even been perpetrated from remote terminals that access the computer over the telephone.

(9) Theft of Time-Sharing Services. When the public is given access to a system, some members of the public often discover how to use the system in unauthorized ways. For example, there are the "phone freakers" who avoid long distance telephone charges by sending over their phones control signals that are identical to those used by the telephone company.

(10) Since time-sharing systems often are accessible to anyone who dials the right telephone number, they are subject to the same kinds of manipulation.

(11) Of course, most systems use account numbers and passwords to restrict access to authorized users. But unauthorized persons have proved to be adept at obtaining this information and using it for their own benefit. For instance, when a police computer system was demonstrated to a school class, a precocious student noted the access codes being used; later, all the student's teachers turned up on a list of wanted criminals.

(12) Perfect Crimes. It's easy for computer crimes to go undetected if no one checks up on what the computer is doing. But even if the crime is detected, the criminal may walk away not only unpunished but with a glowing recommendation from his former employers.

(13) Of course, we have no statistics on crimes that go undetected. But it's unsettling to note how many of the crimes we do know about were detected by accident, not by systematic audits or other security procedures. The computer criminals who have been caught may have been the victims of uncommonly bad luck.

(14) For example, a certain keypunch operator complained of having to stay overtime to punch extra cards. Investigation revealed that the extra cards she was being asked to punch were for fraudulent transactions. In another case, disgruntled employees of the thief tipped off the company that was being robbed. An undercover narcotics agent stumbled on still another case. An employee was selling the company's merchandise on the side and using the computer to get it shipped to the buyers. While negotiating for LSD, the narcotics agent was offered a good deal on a stereo!

(15) Unlike other embezzlers, who must leave the country, commit suicide, or go to jail, computer criminals sometimes brazen it out, demanding not only that they not be prosecuted but also that they be given good recommendations and perhaps other benefits, such as severance pay. All too often, their demands have been met.

(16) Why? Because company executives are afraid of the bad publicity that would result if the public found out that their computer had been misused. They cringe at the thought of a criminal boasting in open court of how he juggled the most confidential records right under the noses of the company's executives, accountants, and security staff. And so another computer criminal departs with just the recommendations he needs to continue his exploits elsewhere.

**Реферат**

Все больше и больше, операций наших предприятий, правительства, и финансовых учреждений управляются информацией, которая существует только в компьютерной памяти. Каждый достаточно умный может модифицировать эту информацию для своих собственных целей, и могут снимать хороший урожай. И что хуже, целому ряду людей, которые совершили это и были пойманы при этом удалось остаться без наказания.

Банковское дело. Все кроме самых маленьких банков теперь сохраняют свои учетные записи в компьютерных файлах. Кто-то, кто знает, как изменить числа в файлах, может перемещать средства по своему желанию. Например, один программист был пойман, перемещая средства с одних учетных записей на текущий счет его жены.

Бизнес. Компании, которые широко используют компьютеры, предлагают много возможностей и нечестным сотрудникам и умным посторонним. Например, вор имея компьютер, может отправлять продукты компании по адресам на его усмотрение. Или может выпускать чеки, он или его сообщники для мнимых поставок или услуг. Люди сделавшие это было пойманы.

Конечно, мы не имеем никакой статистики по преступлениям, которые были необнаруженными. Но обратите внимание, многие из преступлений, которые мы знаем были обнаружены случайно, а не систематическими ревизиями или другими процедурами безопасности. Компьютерные преступники, которые были пойманы, возможно, были жертвами необыкновенной неудачи.

**Abstract**

This article is about computer crimes.

Anyone clever enough to modify this information for his own purposes can reap substantial re wards. Even worse, a number of people who have done this and been caught at it have managed to get away without punishment. For instance, one programmer was caught having the computer transfer funds from other people's accounts to his wife's checking account. For instance, a thief can have the computer ship the company's products to addresses of his own choosing. Of course, we have no statistics on crimes that go undetected.

This article may be interesting for students cybersecurity