5. Лазарева Н. Проблемы квалификации преступлении в области информатики и электросвязи//Закон и жизнь. -2007. -№12. – С.49-56.
6. Лосев В. Преступления против информационной безопасности //Судовы весник. -2002. -№1. – С.40-46.
7. Рыженкова, О.Ю. Информационная безопасность: определение понятия, место в системе национальной безопасности//Закон и право. -2009. -№1. – С.50-51.
8. Теодор Н.Цырдя. Информационная безопасность в условиях информатизации общества http://security.ase.md/publ/ru/pubru06.html

ОРГАНИЗАЦИЯ ПРОГРАММНО- АППАРАТНОЙ ЗАШИТЫ ИНФОРМАЦИИ ОТ ИНСАЙДЕРОВ

Зинаида Гулка, Ольга Гешова,
Славянский университет (Республика Молдова)

In work the problem of distribution of insider trade is considered by the information. The set of software and tools for protection of the data with the short description of functionality of each utility is presented.

Важнейшей проблемой, стоящей перед руководством и службой безопасности любого предприятия, является проблема лояльности сотрудников, или, иными словами, проблема защиты информации от инсайдеров.[1] Существует множество ролей, приписываемых инсайдеру. Например, в финансовой деятельности незаконные инсайдерские торговые операции с ценными бумагами на основе внутренней информации о деятельности компании-эмитента. Обычно инсайдерами являются директора и старшие менеджеры, а также владельцы более 10 % голосов компании. Очевидно, что обиженный или недовольный сотрудник компании, имеющий легальный доступ к сетевым и информационным ресурсам и обладающий определенными знаниями о структуре корпоративной сети, может нанести своей компании гораздо больший ущерб, чем хакер, взламывающий корпоративную сеть через Интернет.

Более того, в результате ошибки или невнимательности инсайдером может оказаться и вполне лояльный сотрудник, который, например, может вынести из офиса диск с конфиденциальной информацией для того, чтобы поработать дома, и

потерять его или отправить письмо по электронной почте не тому адресату, для которого оно предназначено [2]. Серьезность проблемы инсайдеров подтверждается очередным ежегодным исследованием Института компьютерной безопасности CSI, Computer Security Institute. По результатам этого исследования, в 2007 году количество инцидентов с участием инсайдеров впервые вышло на первое место, обогнав таких традиционных лидеров в этой области как вирусы и кражи ноутбуков: 59% признали угрозой № 1 инсайдеров, 52% - вирусы и 50% - потерю мобильного носителя (ноутбука, флэш-накопителя).[9-11]

Проведенное исследование рынка ПО позволяет выделить следующий набор программных средств и инструментов для защиты данных:

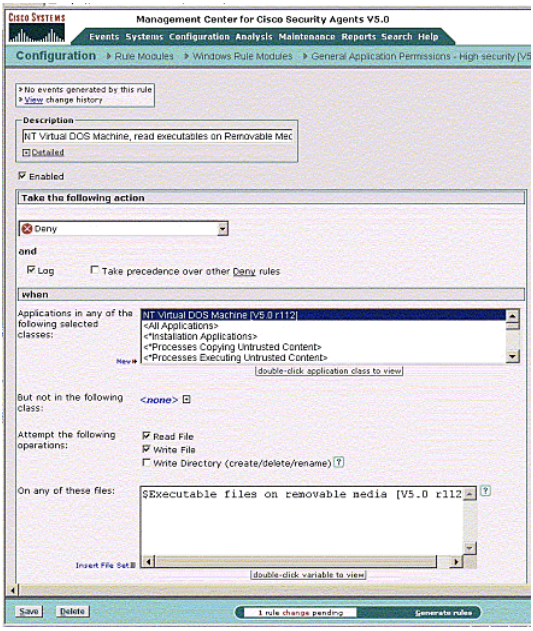

Рис. 1. **Окно программы CSA**

➘ **Cisco Security Agent (CSA)** – объединяет в одном решении различные защитные механизмы и функции по предотвращению атак, защиты от вредоносного кода, блокирования утечки информации через USB-порты и другие внешние устройства. CSA позволяет отражать широкий спектр нападений – сканирование портов, переполнение буфера, троянцев и червей и др. Это, в свою очередь, обеспечивает защиту компью-

тера от неизвестных атак, сигнатуры для которых пока не определены и отсутствуют в базах традиционных средств защиты [7].

➘ **Cryptic Disk** – приложение позволяет легко и надежно зашифровать диски и отдельные разделы на винчестере, защитив их от несанкционированного доступа паролем. При этом вся информация, находящаяся на защищённом диске или записываемая на него, будет автоматически шифроваться. При запуске операционной системы зашифрованный диск/раздел не виден до тех пор, пока он не будет активирован пользователем с помощью пароля доступа в программе Cryptic Disk [3].

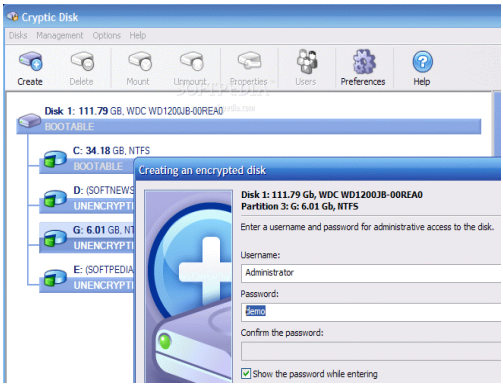

***Рис. 2.* Окно программы Cryptic Disk**

➘ **Safe'n'Sec** – программный модуль, выгодно отличается от большинства приложений, предназначенных для обеспечения безопасности. Следит за активностью разнообразных приложений, процессов, а также за атаками

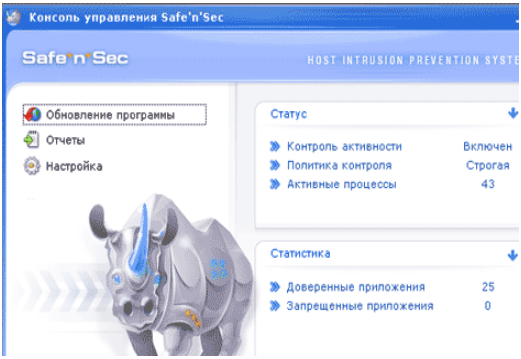

***Рис. 3.* Окно программы Safe'n'Sec**

извне и блокирует любые потенциально опасные действия, анализируя не код приложений, а их активность. Например, она пресекает попытки изменения системных файлов, добавления в реестр новых данных, открытия сетевого соединения для разнообразных приложений и т.д. Таким образом, Safe'n'Sec может защитить даже от самых новых вирусов, которые еще не были созданы на момент установки программы на компьютер [4].

➘ **Zlock** – утилита для защиты от копирования информации на мобильные накопители. Программа предназначена для разграничения доступа к устройствам и обеспечения реализации правил на разрешение или блокирование доступа в соответствии с заданными политиками доступа клиента и администратора. Например: разграничение/блокирование доступа к устройствам, запись событий и др. [5-6].

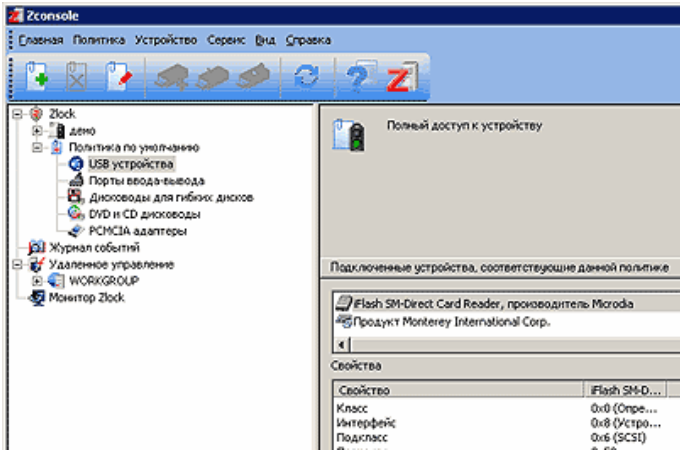

Рис. 4. **Окно программы Zlock**

Наряду с использованием готовых программных продуктов, описанных выше следует рекомендовать: для организации правильной системы разграничения доступа к информации - применение матричного разграничения доступом ко всем электронным файлам и документам предприятия; для защиты операционной системы каждой рабочей станции предприятия – использование всеми сотрудниками в обязательном порядке сложного, трудноподбираемого пароля от 8 символов для санкционированного входа в систему; для правильной работы ОС на всех рабочих станциях фирмы - отключение неиспользуемых служб для защиты компьютеров от внешних угроз [8].

Литература

1) Балина И.В., Гулка З.Н. Защита информации в экономических информационных системах Региональные и международные аспекты К.: Слав. ун-т., 2007. - 125 с.
2) Грушо А. А., Тимонина Е. Е. Теоретические основы защиты информации. М.: Яхтсмен, 2006, с. 192 – 199.
3) Козырев А.А. Информационные технологии в экономике и управлении: Учебник /А.А.Козырев. –СПб.: Изд-во Михайлова В.А., 2000. – 360 с.
4) Конев И.Р., Беляев А.В. Информационная безопасность предприятия. – СПб.: БХВ-Петербург, 2003. – 752 с.
5) Мельников В. Защита информации в компьютерных системах. – М.: Электроинформ, 2005.- 102 с.
6) http://www.securit.ru/products/info/zlock/
7) http://www.lwcom.ru/solutions/doc.php?do=read&doc=72
8) http://www.surfcontrol.ru/products/email/

GESTIUNEA RESURSELOR INFORMAȚIONALE UNIVERSITARE

Constantin Sclifos,
Academia de Studii Economice din Moldova

The report presents and discusses the view according to which the information resources of the university need to design and operation of information security system is designed to ensure confidentiality, integrity and availability of information.

Scopul exploatării sistemelor informaționale în universități este de a optimiza consumul de resurse cheltuite necesare colectării, prelucrării, stocării și furnizării spre consumatori a informațiilor necesare.

Sistemul Informațional (SI) reprezintă prin sine un set de elemente componente interdependente, care colectează, procesează, stochează și difuzează informații pentru a sprijini activitățile organizației.

Sistemele informaționale moderne sunt caracterizate de un set de proprietăți-cheie, care afectează în mod semnificativ securitatea informațională și impun cerințe suplimentare față de sistemul de protecție a informației, printre care:

- sistem cu o structură complexă, format din mai multe sub-