УДК 004.056.53

ОБЕСПЕЧЕНИЕ ИНФОРМАЦИОННОЙ БЕЗОПАСНОСТИ В ВЫЧИСЛИТЕЛЬНОЙ СЕТИ ПРЕДПРИЯТИЯ

Дагаев Александр Федорович
к. т. н., доцент

Самойлов Алексей Николаевич
к. т. н., ассистент

Борисова Елена Александровна
ассистент

Технологический институт ЮФУ, Таганрог, Россия

Средства информационной безопасности программно-аппаратного комплекса вычислительной сети предприятия играют важную роль при реализации общей стратегии и тактики безопасности предприятия. От грамотной реализации принятой политики в области информационной безопасности зависят бесперебойность и устойчивость работы программного и аппаратного обеспечения, конфиденциальность личной информации, степень защиты от несанкционированного доступа для соблюдения коммерческих интересов предприятия. В статье представлены результаты анализа проблем информационной безопасности при использовании информационных технологий.

Ключевые слова: ИНФОРМАЦИОННАЯ БЕЗОПАСНОСТЬ, УТРАТА ИНФОРМАЦИИ, ПРОГРАММНОЕ ОБЕСПЕЧЕНИЕ.

UDC 004.056.53

PROVISION OF INFORMATIONAL SECURITY IN COMPUTER NETWORK OF AN ENTERPRISE

Dagaev Alexander Fedorovich
Cand. Tech. Sci., assistant professor

Samoilov Alexey Nikolaevich
Cand. Tech. Sci., lecturer

Borisova Elena Alexandrovna
lecturer

Technological institute of SFU, Taganrog, Russia

Means of information safety of a hardware-software complex of the computer network of an enterprise play an important role at the realization of the general strategy and tactics of the enterprise safety. Uninterrupted operation and stability of a program work and hardware maintenance, confidentiality of the personal information, a degree of protection against non-authorized access depend on competent realization of the accepted policy in the field of information safety for observance of commercial interests of an enterprise. Results of the problems analysis of information safety at use of information technologies are presented in this paper.

Key words: INFORMATIONAL SECURITY, LOSS OF INFORMATION, SOFTWARE.

Определения

Информационная безопасность (ИБ) – комплекс мероприятий и средств по обеспечению сохранности информации, находящейся в информационной системе, передаваемой, обрабатываемой, хранимой и предоставляемой системой.

КИС – корпоративная информационная сеть;

РС – рабочая станция;

ПО – программное обеспечение.

Назначение системы информационной безопасности состоит в организации безопасных и надежных: мероприятий по доступу к

информации, способов передачи и хранения информации, методов работы с информацией, правил управления доступом к информации, способов восстановления информации, методов резервирования информации.

Задача системы информационной безопасности обуславливается ее назначением и состоит в: обеспечении безопасного, надежного хранения и передачи информации в электронном виде, расположенной на различных носителях; организации надежного доступа к электронной информации; ограничении и контроле доступа к информации, с которой работают сотрудники; создании правил безопасной работы с информацией; проведении мероприятий по резервированию информации; обеспечении восстановления информации в аварийных ситуациях; поддержании информационной безопасности на заданном уровне (рисунок 1).

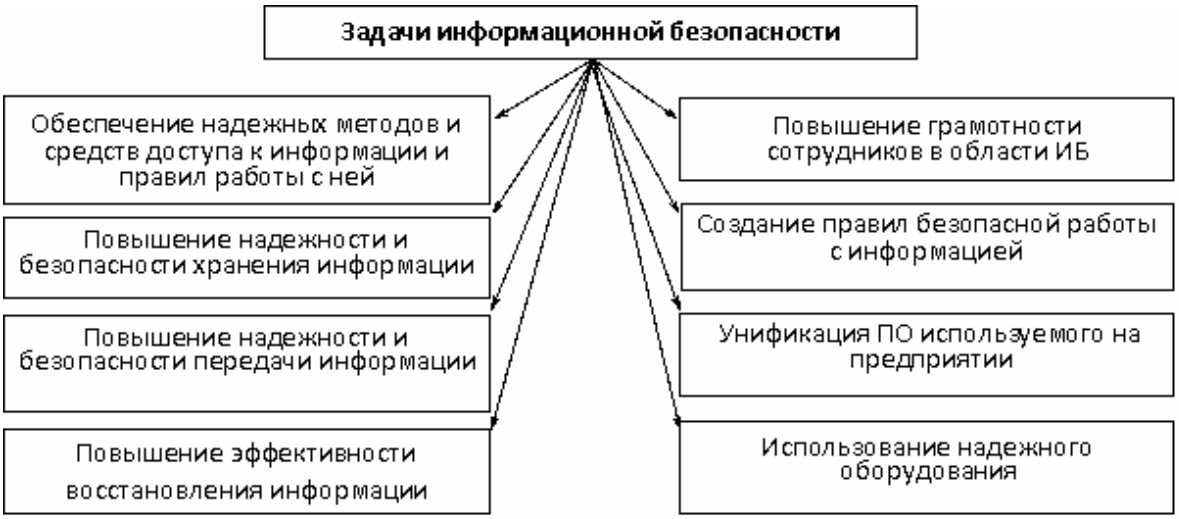

Рис.1 Задачи системы информационной безопасности КИС

1. Причины утраты информации и способы их устранения

Информация может быть утеряна вследствие причин различного вида. Рассмотрим причины потери информации, хранимой на PC и серверах, циркулирующей в сети (рисунок 2). Причины могут быть разделены на несколько групп. Они могут быть внешние и внутренние, внешние причины вызваны внешним воздействием на информацию.

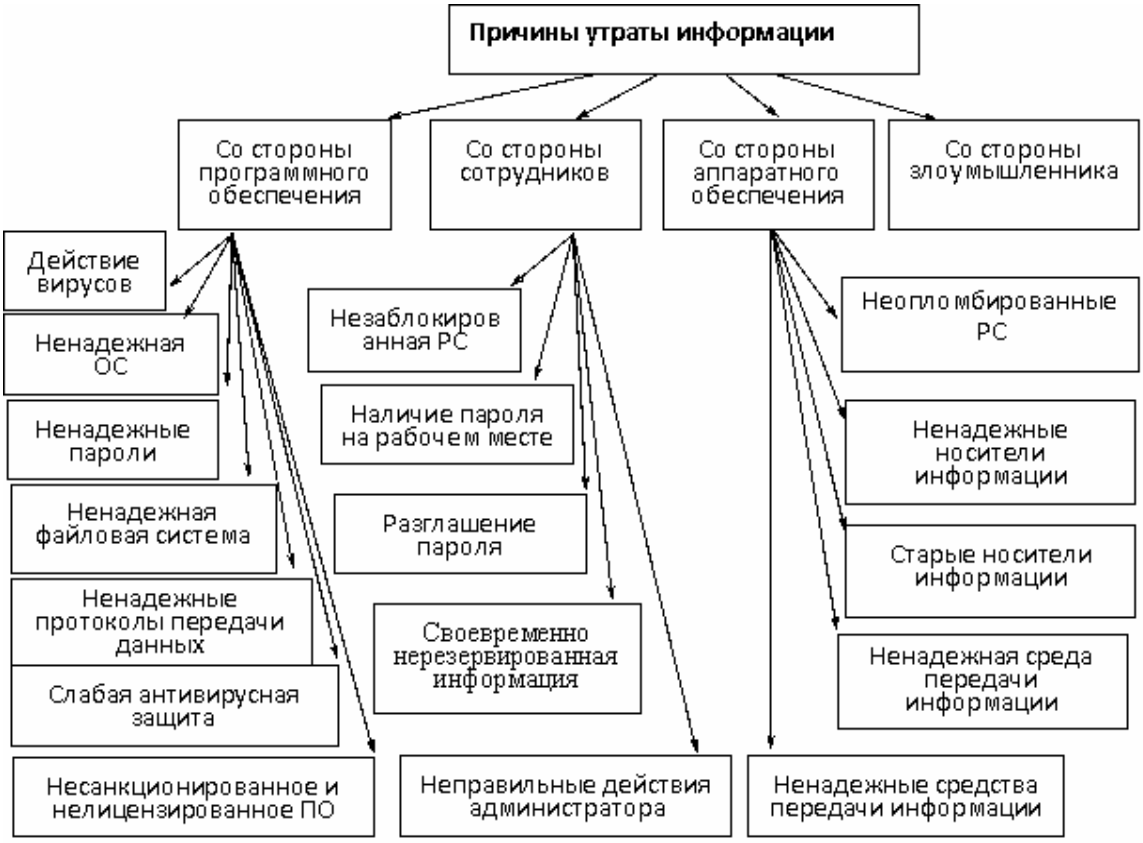

Рис.2 Классификация причин утраты информации, размещенной на РС

К внешним причинам относятся действие злоумышленника и вирусное воздействие. Внешнее воздействие обуславливается попытками сторонних лиц получить доступ к конфиденциальной информации, причины подобных попыток могут быть разнообразны. Воздействие вирусов может стать причиной: несанкционированной передачи информации по сети; удаления данных с компьютера, изменения данных, форматирования жесткого диска.

Внутренние причины – это причины воздействия на информацию программного обеспечения, сотрудников и аппаратного обеспечения. Причина утраты вследствие ненадежности паролей обусловлена их простотой и недостаточным числом символов. Устранение этой причины должно осуществляться системным администратором.

Периодическое обновление антивирусных баз является обеспечением защиты от действия вирусов. Нелицензированное использование ПО может привести к появлению в системе открытых портов, порче системной информации, неправильному использованию ОС, конфликтным ситуациям между приложениями и зависанию системы.

Действия сотрудников могут быть причиной потери ценной информации. Например, РС надо блокировать во время отсутствия сотрудника на рабочем месте, в противном случае, любое стороннее лицо может воспользоваться его данными.

Со стороны аппаратного обеспечения несанкционированный доступ к РС может быть осуществлен, если РС не опломбирована.

2. Отрицательное воздействие на информацию

Рассмотрим типы отрицательных воздействий, которые могут быть осуществлены с информацией, хранимой на РС и серверах (рисунок 3).

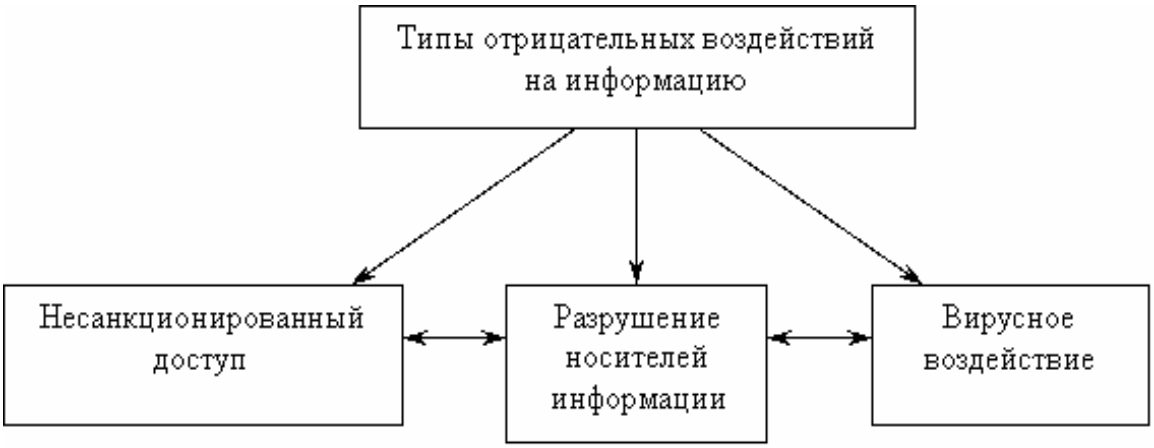

Рис.3 Отрицательные воздействия на информацию

В общем случае отрицательные воздействия можно разбить на три функционально обособленные группы. Воздействия, входящие в первую группу, связаны с несанкционированным доступом.

Разрушение носителей информации может происходить вследствие

старения оборудования, некачественного производства, изменения условий работы на критические и т.д. К носителям информации в данном случае можно отнести: жесткие диски, стримеры, CD диски, дискеты, DVD диски, MO диски и другие устройства хранения.

Третий тип внешних воздействий основан на действии вирусных программ, которые позволяют изменять, передавать и удалять информацию с PC. На рисунке 3 двунаправленными стрелками показано, что все типы отрицательных воздействий связаны между собой, то есть одни типы могут приводить к появлению других.

3. Программные средства обеспечения безопасности компьютерных систем

Следуя процессу загрузки, первым средством защиты является пароль на вход в BIOS. (Basic Input/Output system). Пароль, который используется перед загрузкой системы, также сохраняется в BIOS. Дальнейшим уровнем защиты информации является пароль, который используется при загрузке ОС. Для определения мощности пароля можно использовать специальное ПО, например LC+4 [1–2].

Следующий уровень защиты представляют системные службы, отвечающие за: права пользователей, выделение ресурсов, установление приоритетов схем запуска процессов и т.д. Следующим уровнем является уровень сетевых приложений и протоколов, отвечающих за сетевое подключение пользователей, правила доступа к сетевым ресурсам и правила их использования. Сканеры безопасности, такие как XSpider и ISS, позволяют определять сетевые и локальные уязвимости PC и серверов [3].

Распространенными средствами пользовательского обеспечения сетевой защиты под операционными системами Windows являются ZoneAlarmPro и Outpost [4]. Для обеспечения антивирусной защиты можно использовать ряд мощных пакетов, таких как: NOD32, TrendMicro и др.

Процесс резервирования информации является важным как для конкретного сотрудника, так и для всего предприятия в целом. Правила резервирования и правила работы со встроенными средствами резервирования представлены в [5–6]. В ряде случаев используются программные пакеты, такие как: Symantec (Veritas) backup, BrightStor ARCserve Backup, Acronis True Emage и др. Средства программного и аппаратного восстановления информации также относятся к средствам, обеспечивающим безопасность информации: Ontrack EasyRecovery Pro, FinalData, GetDataBack for (NTFS, FAT), BadCopy Pro и др. Процесс восстановления является долговременным, трудоемким и требует часто знаний о строении файловой системы.

Вывод

В статье был проведен анализ проблем обеспечения информационной безопасности при использовании информационных технологий и рассмотрены причины утраты информации, представлены программные средства обеспечения информационной безопасности. Анализ компонентов программно-аппаратного сетевого комплекса подтвердил важность и необходимость решения вопросов ИБ, пренебрежение которыми может сказаться на эффективности работы всего предприятия, а также привести к значительным экономическим потерям. Поэтому при внедрении эффективных политик ИБ [6] необходимо выработать четкие правила работы с информацией и строго придерживаться их, проводить разработанные мероприятия по поддержанию и улучшению инфраструктуры информационной среды предприятия, по резервированию и внедрению информации, повышению уровня квалификации персонала в области ИБ.

Список литературы

1. Безмалый, В.Ф. Чем нас пытаются взломать (Краткий обзор программ-взломщиков паролей) / В.Ф. Безмалый, Е.В. Безмалая, 2006. 15 с., www.citforum.ru.

2. Ричард Э. Смит Аутентификация: от паролей до открытых ключей. – М., 2002. – 432 с.

3. Редакция журнала 3DNews Сравнение сетевых сканеров безопасности, 2007, http://www.3dnews.ru.

4. Оглтри Т. Firewalls. Практическое применение межсетевых экранов, ДМК Пресс, 2003.

5. Астахов А. Разработка эффективных политик информационной безопасности // IT Директор. – 2005. – январь.

6. Филиппов М.В. Проблемы защиты и резервирования информации в современных информационных системах, 2006, http://www.kacha.ru.