НАУКОВО-ТЕХНІЧНИЙ ЖУРНАЛ «ЗАХИСТ ІНФОРМАЦІЇ» №1, 2008
УДК.004. 621:681.3.06
Коженевський С.Р.

НОВЫЙ ПОДХОД К ЗАЩИТЕ ИНФОРМАЦИИ В ПЕРСОНАЛЬНЫХ КОМПЬЮТЕРАХ

В открытых отечественных и зарубежных публикациях достаточно подробно рассмотрены и классифицированы технические каналы утечки информации, образуемые при обработке информации с ограниченным доступом на персональных компьютерах (ПК). [1]

Развитие рыночных отношений в Украине обострило проблему безопасности информации, при этом одновременно стали стремительно развиваться два процесса:

- первый, по защите информационных ресурсов;
- второй, по добыванию информации или причинения ей ущерба, вплоть до ее уничтожения.

Тенденции развития современного мира характеризируются созданием единого глобального информационного пространства на планете, а, следовательно, проблема информационной безопасности становится проблемой коллективной, а не отдельно взятой страны или организации.

В настоящее время сформирована государственная задача по обеспечению противодействия техническим разведкам. Было введено понятие – канал утечки информации. В отношении ПК основное внимание уделяется следующим каналам [2]:

- прямое похищение носителей информации (в том числе копирование информации, находящей на носителях);
- несанкционированное подключение к аппаратуре и линиям передачи данных или незаконное использование зарегистрированных терминалов пользователей;
- несанкционированный доступ к информации за счет специального приспособленного математического и программного обеспечения;
- перехват электронного излучения с информационными (опасными) сигналами при обработке информации.

Для предотвращения утечки информации необходимы специальные мероприятия, методы и средства. При этом наибольшее внимание уделяется:

- программным средствам;
- программно-аппаратным средствам;
- пассивному методу - экранированной фильтрации.

На достоинствах и недостатках прежней концепции противодействию техническим разведкам не будем останавливаться, так как это достаточно полно освещено в литературе. Однако, следует отметить, что активный метод (зашумление) разрабатывается интенсивнее и быстрее внедряется, так как не требует серьезных финансовых затрат при постановке на производство.

Процесс так называемой переходной экономики сгенерировал создания структур негосударственной собственности, занимающихся проблемами безопасности информации, в которые пришли опытные специалисты из госструктур. Доступнее стали и высокие технологии, и публикации по проблеме защиты информации. Эти факторы стимулировали ускоренное развитие целого ряда методов, способов и средств защиты информации.

Следует отметить, что согласно нормативным документам перечень сведений, разглашение которых может нанести вред интересам собственника информационных ресурсов, это:

1. В сфере основной деятельности:
   - сведения о научно-производственных возможностях;
   - сведения о планах развития предприятия и методах управления;
   - обьем закупок и продаж.
2. В сфере финансов:
   - банковские счета и операции;

- международные расчеты;
- источники и размеры кредитов.

3. В сфере партнерских отношений:
   - списки контрагентов и сведения об их финансовом состоянии;
   - сведения о подготовке переговоров, включая тематику их ведения.

Перечисленные объемы информации хранятся, обрабатываются в ПК и передаются по линиям связи абонентов. Поэтому, если не приняты необходимые и достаточные меры по предотвращению утечки информации по каналам, образованным средствами ВТ, то ни о какой защите информации не может идти речи – т.е. несанкционированный доступ к ней возможен.

В настоящее время в концепции технической защиты информации появились дополнительные требования по:

- аутентификации, достоверности и целостности информации;
- биологической защите информации;
- противодействию электромагнитному терроризму и т.д.

Расширение спектра требований, которые необходимо учитывать при проектировании и изготовлении ПК в специсполнении, вызвало изменения в концепции защиты информации. Например, при применении активного метода защиты необходимо понимать суть его негативного воздействия для решения задачи обеспечения биологической защиты оператора.

Электромагнитное излучение имеет следующие факторы воздействия на организм человека:

- биологический;
- специфический (биохимическое изменение);
- тепловой (локальный нагрев тканей),

что приводит к профзаболеваниям.

При выборе метода, обеспечивающего комплексное предотвращение утечки информации, необходимо учитывать следующие требования:

- гарантированное обеспечение требуемого уровня защиты информации;
- биологическую защиту оператора;
- защиту от электромагнитного терроризма;
- технологическую пригодность к серийному производству;
- сохранение дизайна ПК.

В наибольшей степени удовлетворяет этим требованиям только пассивный метод защиты информации. В общем случае – это локализация источников побочных электромагнитных излучений, т.е. экранирование и фильтрация тононесущих цепей.

Полное и безвозвратное исчезновение отечественного производителя ПК, элементарной базы и ориентация на поставку комплектующих и ПК зарубежных производителей потребовало новых подходов в решении вопросов по защите информации.

Таким образом появилась необходимость в разработке нового подхода, который обеспечивал бы функции защищенности информации, обрабатываемой на ПК, любого состава, структуры построения, назначения, геометрических форма и размеров, при сохранении всех, эксплуатационных характеристик, дизайна и был бы свободен от всех недостатков.

Новый подход к решению задач защиты информации базируется на пассивном методе (экранирование и фильтрация), но в отличие от прежних универсальных вариантов его применения, предлагается индивидуальный подход к закрытию каналов утечки информации. В основу индивидуального подхода положен анализ устройств и комплектующих ПК с целью определения общих конструктивных и схемотехнических решений исполнения, определения параметров побочных излучений и на основании анализа этих данных осуществляются мероприятия по защите.

В общем случае ПК состоит из:

- системного блока;
- монитора;
- клавиатуры;
- манипулятора (мышь);
- принтера;
- акустической системы.

Анализ конструктивного исполнения ПК позволяет определить у них обобщенные признаки подобия (ОПП) и различия в зависимости от функционального назначения.

Системный блок. Большое многообразие корпусов вертикального и горизонтального исполнения.

ОПП: каркас, кожух, передняя панель, органы управления и индикации, блок питания и ввод-вывод коммутаций.

Монитор. Различные геометрические формы корпусов из пластмассы, три типа экранов: плоский, цилиндрический и с двумя радиусами кривизны в различных плоскостях.

ОПП: пластмассовые корпусные детали, ввод коммуникаций, органы управления и сигнализации.

Клавиатура. Незначительные различия в геометрии корпусов из пластмассы (у некоторых типов поддон из метала).

ОПП: пластмассовые корпусные детали, ввод коммуникаций и органы сигнализации.

Манипулятор (мышь). Незначительные различия в геометрии корпусных деталей из пластмассы.

ОПП: пластмассовые корпусные детали, ввод коммуникаций.

Принтер (лазерный, струйный). Корпуса различной геометрии из пластмассы, органы управления и различные разъемные соединения.

ОПП: пластмассовые корпусные детали, ввод коммуникаций, органы управления и сигнализации.

Акустические системы. Большое многообразие геометрических форм корпусов из пластмассы и дерева.

ОПП: ввод-вывод коммуникаций, органы управления и сигнализации, а для отдельных групп - пластмассовые корпусные детали.

Таким образом, обобщенные признаки подобия образуют три основные группы, присущие базовому составу ПК, с некоторым приходится работать при решении задач защиты информации:

- корпусные детали из пластмассы;
- ввод-вывод коммуникаций;
- органы управления и сигнализации.

При этом учитываются и общесистемные проблемные вопросы :

- разводка и организация электропитания и тип заземления;
- согласование сопротивлений источников и нагрузок;
- блокирование взаимного электромагнитного излучения устройств ПК;
- исключение влияния электростатического поля;
- эргономика рабочего места и т.д.

Следующий этап – это разработка типовых конструкторско – технологических решений, реализация которых направлена на предотвращение утечки информации за счет расширения функций конструктивов устройств ПК. Набор типовых конструкторско-технологических решений варьируется в зависимости от состава устройств в ПК, но для базовой модели ПК с учетом обобщенных признаков подобия он содержит решения по :

- металлизации внутренних поверхностей деталей из пластмассы;
- экранированию проводных коммуникаций;
- согласованию сопротивлений источников и нагрузок;
- экранированию стекол для монитора и изготовлению заготовок различных форма из стекол;

- фильтрации сетевого электропитания и его защите от перенапряжений;
- нейтрализация влияния электростатического поля;
- расположению общесистемных проводных связей;
- точечная локализация электромагнитных излучений;
- исключению электромагнитных излучений органами управления и сигнализации;
- разногерметизирующим уплотнителям из различных материалов;
- исключению взаимного влияния электромагнитного излучения устройств ПК.

На основании вышеизложенного разрабатываются технические требования по защите информации в конкретном составе ПК. Практика выложенных в ООО "ЕПОС" опытно-конструкторских работ по изготовлению ПК с системой защиты информации показали, что реализация таких конструкторско-технологических решений удовлетворят техническим требованиям и нормативной документации по предотвращению утечки информации.

В заключении необходимо отметить, что желание обеспечить, высокоэффективную систему безопасности вполне оправдано, но это требует значительных финансовых затрат. Вместе с тем большие затраты на защиту не всегда адекватны гарантированной системы надежности защиты. Чтобы избежать "саморазорения" от чрезмерных затрат на обеспечение безопасности информации, следует придерживаться принципа необходимой достаточности, т.е. стоимость защиты не должна превышать риска [3] ущерба от негативного воздействия на информационные ресурсы.

Список литературы

1. *Коженевский С.Р., Солдатенко Г.Т.* Предотвращение утечки информации по техническим каналам персонального компьютера. // Захист інформації,№2, 2002.-с.32-37.

2. *Чеховский С.А..* Концепция построения компьютеров, защищенных от утечки информации по каналам электромагнитного излучения.- Информационная безопасность офиса. Научно-практический сборник. К.: ООО "ТИД"ДС" Вып.1. 2003.-с.38-43.

3. *Браіловський М.М., Коженевський С.Р.* та інші. Технічний захист інформації на об'єктах інформаційної діяльності. / За ред. проф. В.О. Хорошка.- К.:ДУІКТ, 2007.-178с.

Надійшла 20.12.2007р.

УДК 539.1.08:539.1.075

Бісик А.М., Дудикевич В.Б.,
Максимович В.М., Смук Р.Т.,
Сторонський Ю.Б., Хорошко В.О.

СУЧАСНИЙ ПРИЛАД РАДІАЦІЙНОЇ РОЗВІДКИ

Радіаційні методи отримання інформації - це порівняно новий метод розвідки що ґрунтується на матеріально-речовинному каналі просочування інформації. Він складає цілий комплекс заходів, які включають як агентурні заходи, так і застосування технічних засобів.

До агентурних відносяться попереднє опрацьовування об'єкту з подальшим відбором проб для проведення лабораторних досліджень.

До технічних засобів відносяться: космічна розвідка, проведення експрес-аналізів об'єкту і дослідження проб в лабораторії, які узяті поблизу об'єкту. Для проведення технічної розвідки широко використовуються дозиметри і радіометри.

Просочування інформації про радіоактивні речовини здійснюється в результаті виносу радіоактивних речовин співробітниками підприємства, переміщення їх по території держави, спроби перевозу через державний кордон або реєстрації зловмисника з радіоактивною речовиною по його випромінюванню за допомогою відповідних приладів. Розвідка ведеться активно, безперервно і своєчасно, а розвіддані повинні бути достовірні.