УДК 004.725.5

ПУТИ И МЕТОДЫ ЗАЩИТЫ ИНФОРМАЦИИ В ЛОКАЛЬНЫХ КОМПЬЮТЕРНЫХ СЕТЯХ
ЛОКАЛДЫК КОМПЬЮТЕРДИК СЕТТЕГИ МААЛЫМАТТАРДЫ КОРГООНУН ЖОЛДОРУ ЖАНА УСУЛДАРЫ
THE WAYS AND METHODS OF PROTECTION INFORMATION IN LOCAL COMPUTING SET

Иванов Ю. – преподаватель,
Аксыйский колледж, ЖАГУ edward_1988@bk.ru

Аннотации: Проблемы защиты информации в локальных компьютерных сетях постоянно находятся в центре внимания широкого круга пользователей. Под защитой информации понимается использование специальных средств, методов и мероприятий с целью предотвращения утери информации,

Локалдык компьютердик сеттердеги маалыматтарды коргоо көптөгөн кеңири колдонуучулардын көңүл чордонунда. Маалыматты коргоонун астында биз мааламатты жоготуп албоо үчүн атайын каражаттарды, усулдарды жана иш чараларды түшүнөбүз.

The problems of protection information in local computing set are always constantly in the center of attention among great sphere of users. Under protection of information is understood using of special facilities, methods and actions for the reason preventions lost of information.

Вопрос защиты информации поднимается уже с тех пор, как только люди научились письменной грамоте. Всегда существовала информация, которую должны знать не все. Люди, обладающие такой информацией, прибегали к разным способам ее защиты. Из известных примеров это такие способы как тайнопись, шифрование. В настоящее время всеобщей компьютеризации благополучие и даже жизнь многих людей зависят от обеспечения информационной безопасности множества компьютерных систем обработки информации, а также контроля и управления различными объектами. К таким объектам можно отнести системы телекоммуникаций, банковские системы, системы обработки и хранения секретной и конфиденциальной информации. Для нормального и безопасного функционирования этих систем необходимо поддерживать их безопасность и целостность.

Обилие приемов съема информации противодействует большое количество организационных и технических способов, так называемая специальная защита. Одним из основных направлений специальной защиты является поиск техники подслушивания или поисковые мероприятия. В системе защиты объекта поисковые мероприятия выступают как средства обнаружения и ликвидации угрозы съема информации.

Проблемы защиты информации в локальных вычислительных сетях (ЛВС) постоянно находятся в центре внимания не только специалистов по разработке и использованию этих систем, но и широкого круга пользователей. Под защитой информации понимается использование специальных средств, методов и мероприятий с целью предотвращения утери информации, находящейся в ЛВС. Широкое распространение и повсеместное применение вычислительной техники очень резко повысили уязвимость накапливаемой, хранимой и обрабатываемой в ЛВС информации.

Четко обозначилось три аспекта уязвимости информации:

1. Подверженность физическому уничтожению или искажению.

2. Возможность несанкционированной (случайной или злоумышленной) модификации.

3. Опасность несанкционированного получения информации лицами, для которых она не предназначена.

Следует отметить, что использование USB флеш-накопителей (гибких магнитных дисков) создает условия для злоумышленных действий (подмена, хищение, внесение в систему «компьютерного вируса», несанкционированное копирование информации, незаконное использование сети ЭВМ и др.). Важнейшая мера защиты информации на этом направлении - четкая организация и контроль использования USB флеш-накопителей.

Так же одним из основных средств защиты информации в ЭВМ являются криптографические средства. Они имеют своей задачей защиту информации при передаче по линиям связи локальной сети, хранении на магнитных носителях, а так же препятствуют вводу ложной информации.

Чтобы надежно защитить информацию, система защиты должна регулярно обеспечивать защиту:

1. Системы обработки данных от посторонних лиц.
2. Системы обработки данных от пользователей.
3. Пользователей друг от друга и каждого пользователя от самого себя.
4. Систем обработки от самой себя.

Архитектура ЛВС и технология ее функционирования позволяет злоумышленнику находить или специально создавать лазейки для скрытого доступа к информации, причем многообразие и разнообразие даже известных фактов злоумышленных действий дает достаточные основания предполагать, что таких лазеек существует или может быть создано много. Пути несанкционированного получения информации приведены на рисунке 1.1.

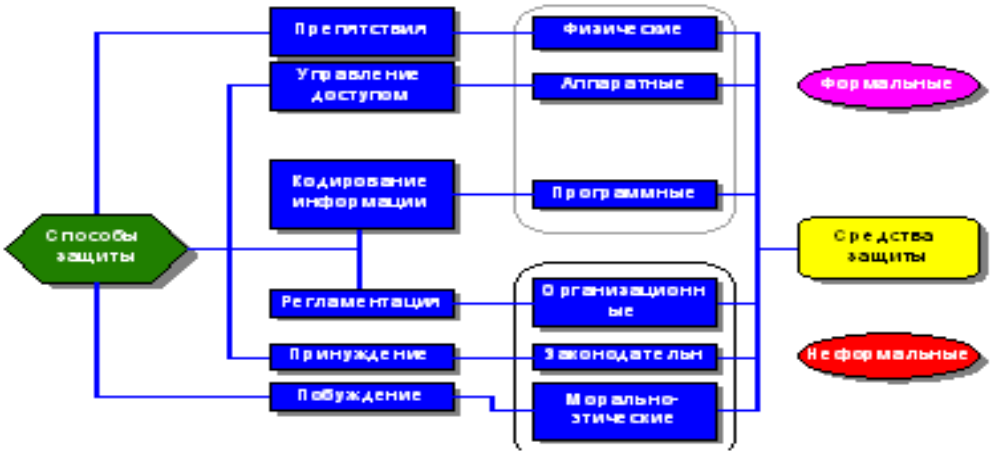

Рисунок 1.1 Способы и средства защиты информации в ЛВС

Несанкционированный доступ к информации, находящейся в ЛВС бывает:

- косвенным - без физического доступа к элементам ЛВС;
- прямым - с физическим доступом к элементам ЛВС.

В настоящее время существуют следующие пути несанкционированного получения информации (каналы утечки информации):

- применение подслушивающих устройств;
- дистанционное фотографирование;

- перехват электромагнитных излучений;
- хищение носителей информации и производственных отходов;
- считывание данных в массивах других пользователей;
- копирование носителей информации;
- несанкционированное использование терминалов;
- маскировка под зарегистрированного пользователя с помощью хищения паролей и других реквизитов разграничения доступа;
- использование программных ловушек;
- получение защищаемых данных с помощью серии разрешенных запросов;
- использование недостатков языков программирования и операционных систем;
- преднамеренное включение в библиотеки программ специальных блоков типа “троянских коней”;
- незаконное подключение к аппаратуре или линиям связи вычислительной системы;
- злоумышленный вывод из строя механизмов защиты.

Для решения проблемы защиты информации основными средствами, используемыми для создания механизмов защиты принято считать:

1. Технические средства - реализуются в виде электрических, электромеханических, электронных устройств. Технические средства подразделяются на:

- аппаратные - устройства, встраиваемые непосредственно в аппаратуру, или устройства, которые сопрягаются с аппаратурой ЛВС по стандартному интерфейсу (схемы контроля информации по четности, схемы защиты полей памяти по ключу, специальные регистры);
- физические - реализуются в виде автономных устройств и систем (электронно-механическое оборудование охранной сигнализации и наблюдения. Замки на дверях, решетки на окнах). Программные средства - программы, специально предназначенные для выполнения функций, связанных с защитой информации.

В ходе развития концепции защиты информации специалисты пришли к выводу, что использование какого-либо одного из выше указанных способов защиты, не обеспечивает надежного сохранения информации. Необходим комплексный подход к использованию и развитию всех средств и способов защиты информации.

Способы защиты информации представлены на рисунке 1.2.

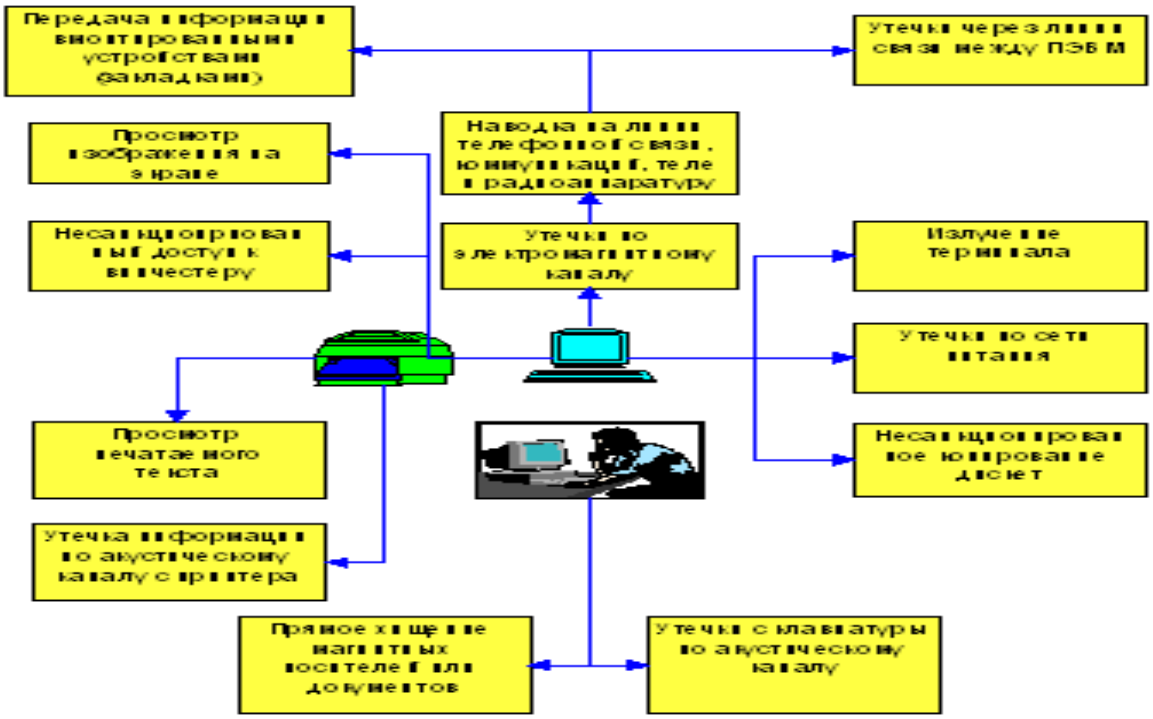

Рисунок 1.2 Основные каналы утечки информации при ее обработке на ПЭВМ

Способы защиты информации в ЛВС включают в себя следующие элементы:

1. Препятствие - физически преграждает злоумышленнику путь к защищаемой информации (на территорию и в помещения с аппаратурой, носителям информации).

2. Управление доступом - способ защиты информации регулированием использования всех ресурсов системы (технических, программных средств, элементов данных).

Управление доступом включает следующие функции защиты:

- идентификацию пользователей, персонала и ресурсов системы, причем под идентификацией понимается присвоение каждому названному выше объекту персонального имени, кода, пароля и опознание субъекта или объекта по предъявленному им идентификатору;
- проверку полномочий, заключающуюся в проверке соответствия дня недели, времени суток, а также запрашиваемых ресурсов и процедур установленному регламенту;
- разрешение и создание условий работы в пределах установленного регламента;
- регистрацию обращений к защищаемым ресурсам;
- реагирование (задержка работ, отказ, отключение, сигнализация) при попытках несанкционированных действий.

3. **Маскировка** - способ защиты информации в ЛВС путем ее криптографического преобразования. При передаче информации по линиям связи большой протяженности криптографическое закрытие является единственным способом надежной ее защиты.

4. **Регламентация** - заключается в разработке и реализации в процессе функционирования ЛВС комплексов мероприятий, создающих такие условия автоматизированной обработки и хранения в ЛВС защищаемой информации, при которых возможности несанкционированного доступа к ней сводились бы к минимуму. Для эффективной защиты необходимо строго регламентировать структурное построение ЛВС

(архитектура зданий, оборудование помещений, размещение аппаратуры), организацию и обеспечение работы всего персонала, занятого обработкой информации.

5. **Принуждение** - пользователи и персонал ЛВС вынуждены соблюдать правила обработки и использования защищаемой информации под угрозой материальной, административной или уголовной ответственности.

Рассмотренные способы защиты информации реализуются применением различных средств защиты, причем различают технические, программные, организационные, законодательные и морально-этические средства.

Организационными средствами защиты называются организационно-правовые мероприятия, осуществляемые в процессе создания и эксплуатации ЛВС для обеспечения защиты информации. Организационные мероприятия охватывают все структурные элементы ЛВС на всех этапах: строительство помещений, проектирование системы, монтаж и наладка оборудования, испытания и проверки, эксплуатация.

К законодательным средствам защиты относятся законодательные акты страны, которыми регламентируются правила использования и обработки информации ограниченного доступа и устанавливаются меры ответственности за нарушение этих правил.

К морально-этическим средствам защиты относятся всевозможные нормы, которые сложились традиционно или складываются по мере распространения вычислительных средств в данной стране или обществе. Эти нормы большей частью не являются обязательными, как законодательные меры, однако несоблюдение их ведет обычно к потере авторитета, престижа человека или группы лиц.

Рассмотренные выше средства защиты подразделяются на:

1. формальные - выполняющие защитные функции строго по заранее предусмотренной процедуре и без непосредственного участия человека.

2. неформальные - такие средства, которые либо определяются целенаправленной деятельностью людей, либо регламентируют эту деятельность.

Обеспечение надежной защиты информации предполагает:

1. Обеспечение безопасности информации в ЛВС это есть процесс непрерывный, заключающийся в систематическом контроле защищенности, выявлении узких и слабых мест в системе защиты, обосновании и реализации наиболее рациональных путей совершенствования и развития системы защиты.

2. Безопасность информации в ЛВС может быть обеспечена лишь при комплексном использовании всего арсенала имеющихся средств защиты.

3. Надлежащую подготовку пользователей и соблюдение ими правил защиты.

Ни одна система защиты не считается абсолютно надежной. Надо исходить их того, что может найтись такой искусный злоумышленник, который отыщет лазейку для доступа к информации.

Литературы:

1. Хорев П. Б. Методы и средства защиты информации в компьютерных системах. – М.: Академия, 2006. – 430 с. - ISBN: 5-908916-87-8
2. Материалы сайта «Защита информации и Информационная безопасность». [Электронный ресурс]. - Режим доступа: http://www.zashita-informacii.ru
3. Барсуков В.С. Безопасность: технологии, средства, услуги / В.С. Барсуков. – М., 2001 – 496 с.
4. Ярочкин В.И. Информационная безопасность. Учебник для студентов вузов / 3-е изд. – М.: Академический проект: Трикста, 2005. – 544 с.

5. Барсуков В.С. Современные технологии безопасности / В.С. Барсуков, В.В. Водолазский. – М.: Нолидж, 2000. – 496 с., ил.
6. Зегжда Д.П. Основы безопасности информационных систем / Д.П. Зегжда, А.М. Ивашко. - М.: Горячая линия – Телеком, 2000. - 452 с., ил.
7. Компьютерная преступность и информационная безопасность / А.П. Леонов [и др.]; под общ. Ред. А.П. Леонова. – Минск: АРИЛ, 2000. – 552 с.

Рецензент: Раев З.Ж. – к.т.н., доцент