УДК 004.056.53

МЕТОДЫ ЗАЩИТЫ ИНФОРМАЦИИ

Иванникова А.О., студентка гр. БЭс–121, IV курс
Научный руководитель: Дороганов В.С., старший преподаватель
Кузбасский государственный технический университет
имени Т.Ф. Горбачева
г. Кемерово

На сегодняшний день информация является наиболее важным ресурсом, потеря которого влечет за собой ряд неприятных последствий. Утратив, конфиденциальные данные компания подвержена угрозе финансовых потерь, поскольку полученной информацией могут воспользоваться конкуренты или злоумышленники. Для того, чтобы предотвратить столь нежелательные ситуации все современные фирмы и учреждения используют методы защиты информации. Все программисты и специалисты в области построения информационных систем проходят целый курс безопасности информационных систем. Однако всем тем, кто работает с секретными данными необходимо знать виды информационных угроз и технологии защиты.

Несанкционированный доступ злоумышленников к данным является основным видом информационных угроз, для защиты от которых на каждом предприятии создается целая технология. Злоумышленники планируют заранее преступные действия, которые могут осуществляться путем прямого доступа к устройствам или путем удаленной атаки, с использованием специально разработанных для кражи информации программ.

В данном случае секретные материалы не попадают в руки злоумышленников, однако утрачиваются и не подлежат восстановлению либо восстанавливаются слишком долго. Сбои в компьютерных системах могут возникать по следующим причинам:

1. Потеря информации вследствие повреждения носителей – жестких дисков;
2. ошибки в работе программных средств;
3. нарушения в работе аппаратных средств из-за повреждения или износа.

Технология защиты данных базируется на применении современных методов, предотвращающих утечку информации и ее потерю. На сегодняшний день используются следующие основные способы защиты:

1. Препятствие;
2. маскировка;
3. регламентация;
4. управление;
5. принуждение;

6. побуждение.

Данные методы нацелены на построение эффективной технологии защиты информации, при помощи которой исключены потери по причине халатности и успешно отражаются разные виды угроз.

Под препятствием понимается способ физической защиты информационных систем, благодаря которому злоумышленники не имеют возможность попасть на охраняемую территорию.

Маскировка представляет собой способы защиты информации, предусматривающие преобразование данных в форму, не пригодную для восприятия посторонними лицами. Для расшифровки требуется знание принципа.

Управление – способы защиты информации, при которых осуществляется управление над всеми компонентами информационной системы.

Регламентация – важнейший метод защиты информационных систем, предполагающий введение особых инструкций, согласно которым должны осуществляться все манипуляции с охраняемыми данными.

Принуждение – методы защиты информации, тесно связанные с регламентацией, предполагающие введение комплекса мер, при которых работники вынуждены выполнять установленные правила. Если используются способы воздействия на работников, при которых они выполняют инструкции по этическим и личностным соображениям – это побуждение [1].

Способы защиты информации предполагают использование определенного набора средств. Для предотвращения потери и утечки секретных сведений используются следующие средства:

1. Физические;
2. программные и аппаратные;
3. организационные;
4. законодательные;
5. психологические.

Физические средства защиты информации предотвращают доступ посторонних лиц на охраняемую территорию. Основным и наиболее старым средством физического препятствия является установка прочных дверей, надежных замков, решеток на окна. Для усиления защиты информации используются пропускные пункты, на которых контроль доступа осуществляют люди (охранники) или специальные системы. С целью предотвращения потерь информации также целесообразна установка противопожарной системы. Физические средства используются для охраны данных, как на бумажных, так и на электронных носителях.

Программные и аппаратные средства – незаменимый компонент для обеспечения безопасности современных информационных систем. Аппаратные средства представлены устройствами, которые встраиваются в аппаратуру для обработки информации. Программные средства – программы,

отражающие хакерские атаки. Также к программным средствам можно отнести программные комплексы, выполняющие восстановление утраченных сведений. При помощи комплекса аппаратуры и программ обеспечивается резервное копирование информации – для предотвращения потерь.

Организационные средства сопряжены с несколькими методами защиты: регламентацией, управлением, принуждением. К организационным средствам относится разработка должностных инструкций, беседы с работниками, комплекс мер наказания и поощрения. При эффективном использовании организационных средств работники предприятия хорошо осведомлены о технологии работы с охраняемыми сведениями, четко выполняют свои обязанности и несут ответственность за предоставление недостоверной информации, утечку или потерю данных.

Законодательные средства – комплекс нормативно–правовых актов, регулирующих деятельность людей, имеющих доступ к охраняемым сведениям и определяющих меру ответственности за утрату или кражу секретной информации.

Психологические средства – комплекс мер для создания личной заинтересованности работников в сохранности и подлинности информации. Для создания личной заинтересованности персонала руководители используют разные виды поощрений. К психологическим средствам относится и построение корпоративной культуры, при которой каждый работник чувствует себя важной частью системы и заинтересован в успехе предприятия [2].

Для обеспечения безопасности информационных систем сегодня активно используются методы шифрования и защиты электронных документов. Данные технологии позволяют осуществлять удаленную передачу данных и удаленное подтверждение подлинности. Методы защиты информации путем шифрования основаны на изменении информации с помощью секретных ключей особого вида. В основе технологии криптографии электронных данных – алгоритмы преобразования, методы замены, алгебра матриц. Стойкость шифрования зависит от того, насколько сложным был алгоритм преобразования. Зашифрованные сведения надежно защищены от любых угроз, кроме физических. Электронная цифровая подпись – параметр электронного документа, служащий для подтверждения его подлинности. Электронная цифровая подпись заменяет подпись должностного лица на бумажном документе и имеет ту же юридическую силу. Электронная цифровая подпись служит для идентификации ее владельца и для подтверждения отсутствия несанкционированных преобразований. Её использование обеспечивает не только защиту информации, но также способствует удешевлению технологии документооборота, снижает время движения документов при оформлении отчетов.

Проблема защиты информации возникла задолго до разработки компьютерной техники. Появление электронных вычислительных машин

привело данную проблему на новый уровень. Как показывает практика: лучшая защита от нападения – это не допускать ее. Нельзя защитить информацию, ограничившись, только техническими методами. Основным недостатком защиты является человеческий фактор и поэтому надежность системы безопасности зависит от отношения к ней.

Для поддержания защиты на высоком уровне, необходимо постоянно совершенствоваться вместе с развитием современной техники и технологий, так сказать двигаться в ногу со временем [3].

Список литературы:

1. Зайцев А.П., Шелупанов А.А., Мещеряков Р.В. и др. Технические средства и методы защиты информации: Учебник для вузов / ООО «Издательство Машиностроение», 2009 – 508 с
2. Соболь Б.В. Информатика: Учебник. – Ростов–на–Дону: Феникс, 2005. – 448с.
3. Шаньгин В. Ф. Информационная безопасность компьютерных систем и сетей: Учебное пособие. – М.; под ред. ИД «Форум»: Инфра–М, 2008 – 416 с.