Защита информации в автоматизированных системах обработки информации.

Ставер Е.В.
Кафедра математического моделирования сложных систем и анализ данных
Белорусский государственный университет)
Минск, Республика Беларусь
e-mail: mindi1987@mail.ru

***Аннотация*—в этой стать подробно раскрывается проблема защиты информации в автоматизированных системах обработки информации. Приводятся примеры реального использования систем криптозащиты, а так же, приведен анализ современных средств защиты АСОИ.**

Ключевые слова: система; обработка; криптоанализ; информация; шифрование.

I. Введение

В нашем современном мире компьютеризации информационные ресурсы стали одним из наиболее мощных рычагов развития общества. Владение информацией необходимого качества – это и есть залог успеха деятельности ИТ. Существуют вопросы правового обеспечения, лицензирования и сертификации в области криптозащиты [1].

Научные и технические разработки приняли огромные масштабы в области информатизации общества на базе современных средств вычислительной техники, а также современных методов автоматизированной обработки информации. Характерными становятся особенности использования вычислительной техники имеющей удельный вес автоматизированных процедур объеме процессов обработки данных [1].

Нарастающая важность решений, принимаемых в автоматизированном режиме; накопление на носителях больших объемов информации, интеграция в единых базах данных информации различного назначения и различной принадлежности.

II. Организационные средства защиты

К организационным средствам защиты относятся организационно-технические и организационно-правовые мероприятия, осуществляемые в процессе создания и эксплуатации АСОД. Организационные мероприятия охватывают все структурные элементы АСОД и системы защиты на всех этапах их жизненного цикла: строительство помещений, проектирование системы, монтаж и наладка оборудования, испытания и проверка в эксплуатации АСОД [2].

При этом организационные мероприятия играют двойную роль в механизме защиты информации: с одной стороны, позволяют перекрыть значительную часть каналов утечки информации, а с другой обеспечивают объединение всех используемых в АСОД средств в целостный механизм защиты [2].

III. Защита информации

В настоящее время применяется значительное число различных аппаратных средств: терминалы пользователей, устройства группового ввода-вывода данных, центральные процессоры, внешние запоминающие устройства.

В терминалах пользователей наибольшее распространение получили устройства предназначенные для предупреждения несанкционированного включения терминала в работу, обеспечения идентификации терминала (схемы генерирования идентифицирующего кода) и идентификации пользователя (магнитные индивидуальные карточки, дактилоскопические и акустические устройства опознавания и т.п.). Реализация указанных принципов возможна при использовании методов защиты от НСД, включающих, в частности, организационные, технологические и правовые меры и мероприятия [3]. К первой категории относятся средства, регламентируемые внутренними инструкциями организации, эксплуатирующей АС (например, правила и порядок работы с грифованными документами, принятые на данном предприятии). Вторую категорию составляют механизмы защиты, реализуемые на основе аппаратно-программных средств и обеспечивающие как минимум идентификацию, аутентификацию и разграничение прав доступа пользователей. Последняя категория включает механизмы разработки общегосударственной нормативной базы по вопросам защиты информации от НСД и меры по контролю за их выполнением [3]. Несколько слов о системе сертификации продукции по требованиям безопасности информации, которая является составной частью системы сертификации продукции. Под сертификацией продукции по требованиям безопасности информации понимается комплекс организационно - технических мероприятий, в результате которых посредством специального документа - сертификата и знака соответствия с определенной степенью достоверности подтверждается, что продукция соответствует требованиям стандартов по безопасности информации или иных нормативно-технических документов. Указанная система предусматривает сертификацию технических, программно-технических, программных средств, систем, сетей вычислительной техники и связи, средств защиты и средств контроля эффективности защиты по требованиям безопасности

информации. В настоящее время разработан проект "Положения о сертификации средств и систем вычислительной техники и связи по требованиям безопасности информации". При сертификации могут подтверждаться как отдельные характеристики, так и весь комплекс характеристик продукции, связанных с обеспечением безопасности информации. Органы по сертификации и испытательные центры несут ответственность за выполнение возложенных на них функций, обеспечение сохранности государственных и коммерческих секретов, а также за соблюдение авторских прав заявителя при испытаниях его продукции.

Механизмы идентификации и аутентификации тесно связаны. И если первые обеспечивают присвоение пользователям идентификаторов и проверку их корректности при предъявлении, то вторые – проверку принадлежности пользователю предъявленного им идентификатора.

Методы аутентификации различаются по способу хранения и представления информации подтверждения. Обычно они подразделяются на три группы: парольные методы, методы с использованием аппаратно-программных “ключей”, методы биометрической персонификации [4].

Парольные методы получили максимальное распространение. Как правило, они включаются в качестве базовых в большинство аппаратно-программных комплексов защиты информации. Это обусловлено как экономическими причинами, так и хорошо отработанной теорией и практикой создания таких систем. Во вторую группу входят методы аутентификации, использующие носимые устройства для контроля доступа к автоматизированному рабочему месту пользователя (электронные ключи Touch Memory, электронные карты Smart Card, устройства доступа типа “Активатор” и др.). Последнюю группу составляют методы аутентификации, основанные на измерении и сравнении с эталоном индивидуальных характеристик пользователя: отпечатков пальцев (например, оригинальное устройство фирмы “Calspan”), структуры радужной оболочки глаза и т.п. Угрозы, не связанные с деятельностью человека. Наиболее типичной естественной угрозой АСОД, не связанной с деятельностью человека, является, например, пожар. Поэтому при проектировании АСОД целесообразно рассмотреть вопросы противопожарной безопасности. Для зданий, где размещаются технические средства АСОД, расположенных в долинах рек или на побережье, весьма вероятной угрозой является затопление. В этих случаях аппаратные средства АСОД целесообразно устанавливать на верхних этажах зданий и должны приниматься другие меры предосторожности. Нанесение ущерба ресурсам АСОД может произойти в следствии стихийного бедствия. Ущерб может быть нанесен при технических авариях, например, при внезапном отключении электропитания. Гораздо шире класс угроз АСОД и обрабатываемой информации, связанных с деятельностью человека. Требования по управлению доступом занимают одно из основных мест в составе РД ГТК по защите информации от НСД. Главной задачей контроля и управления доступом является определение множества данных и операций над ними, разрешенных для пользователей информационной системы [4]. Основой дискреционного метода является матрица прав доступа, строки которой соответствуют субъектам (пользователи), а столбцы – объектам (файлы, каталоги и т.д.). В ячейках матрицы содержатся права доступа субъектов к объектам. Мандатный принцип разграничения доступа обеспечивает контроль доступа, следуя правилам используемой модели управления доступом на основе сопоставления классификационных меток субъектов и объектов защиты. Для криптографического закрытия информации в АСОД наибольшее распространение имеет шифрование данных. При этом используется несколько различных систем шифрования: заменой, перестановкой, гаммированием.

Широкое распространение получили комбинированные шифры, когда исходный текст последовательно преобразуется с использованием двух или даже трех различных шифров. Основной характеристикой меры защищенности информации криптографическим закрытием является стойкость шифра, причем под стойкостью понимается тот минимальный объем зашифрованного текста.

Таким образом, по значению стойкости системы шифра можно определить допустимый объем шифрования информации при одних и тех же ключевых установках [5].

IV. Заключение

Огромная проблема современной защиты информации и в большей части современного программирования и современной защиты информации является то, что мы имеем массу реальных алгоритмов криптозащиты и можно утверждать, что они совершенны на 98%, но неумение современного программирования и не понимания сути задачи и работы этих алгоритмов программистами, приводит к сомнению в работе алгоритмов. Неумение программно реализовать алгоритм шифрования, не правильное применение технологий программирования, мы сами себя добровольно отдаем в руки хакерам и злоумышленникам, а эти «уникальные» люди, видя и зная наши ошибки, дорабатывают ПО шпионскими модулями получают доступ к данным, которые мы считаем секретными.

[1] Нечаев В.И. Элементы криптографии (Основы теории защиты информации). — М.: Высшая школа, 1999. — 109 с.

[2] Герасименко В. А. Защита информации в автоматизированных системах обработки данных., кн. 1, 2. М.: Энергоатомиздат, 1994.

[3] Основы криптозащиты АСУ. Под ред. Б. П. Козлова. М.: МО, 1996

[4] Мельников В. В. Защита информации в компьютерных системах. М.: Финансы и статистика, 1997