УДК 004.7:65.012.8

ОСОБЕННОСТИ МЕРОПРИЯТИЙ ПО ЗАЩИТЕ ИНФОРМАЦИИ И ИХ УЯЗВИМОСТИ

И.В. РУСАКОВ[1], А.М. ПРУДНИК[2]

[1]ООО «Исток истины»
ул. Геологическая, 117, к. 1, г. Минск, 220138, Республика Беларусь
IstokIstin@tut.by

[2]Белорусский государственный университет информатики и радиоэлектроники
ул. П. Бровки, 6, г. Минск, 220013, Республика Беларусь
aleksander.prudnik@bsuir.by

Приводится обоснование разработки, а также практические аспекты внедрения системы менеджмента информационной безопасности (СМИБ) для государственных учреждений в соответствии со стандартом СТБ ISO/IEC 27001:2011 «Системы менеджмента информационной безопасности. Требования».

Ключевые слова: защита информации, недекларированные возможности, уязвимость.

Для обеспечения конфиденциальности, целостности и доступности информации необходимо обеспечивать функционирования информационных систем, которые создают, хранят и передают данную информацию.

Различают следующие способы получения несанкционированного доступа к информации:

– подслушивание разговоров в помещении или автомашине с помощью предварительно установленных «радиожучков» или диктофонов;

– контроль телефонов, телефонных и прочих линий связи, радиотелефонов и радиостанций;

– дистанционный съём информации с различных технических средств, в первую очередь, с мониторов и печатающих устройств компьютеров и другой электронной техники;

– облучение оконных стекол в помещении, где ведутся «интересные разговоры» или, например, направленное радиоизлучение, которое может заставить «откликнуться и заговорить» детали в телевизоре, в радиоприемнике или другой технике;

– использование недокументированных возможностей в технических и информационных системах (установка расположения, прослушивание).

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.

Под безопасностью информационной системы подразумевается ее защищенность от преднамеренного или случайного несанкционированного доступа и нанесения тем самым вреда нормальному процессу документооборота и обмена данными в системе, а также хищения, модификации и уничтожения информации. Другими словами вопросы защиты информации и защиты информации в информационных системах решаются для того, чтобы изолировать нормально функционирующую информационную систему от несанкционированных управляющих воздействий и доступа посторонних лиц или программ к данным с целью хищения или уничтожения.

Если взять модель, описывающую любую управляемую информационную систему, можно предположить, что возмущающее воздействие на нее может быть случай-

ным. Именно поэтому, рассматривая угрозы безопасности информационным системам, следует сразу выделить преднамеренные и случайные возмущающие воздействия.

Средства защиты информации могут быть выведены из строя, например из-за дефектов аппаратных средств или уязвимости используемых алгоритмов. Также существенное отрицательное воздействие на защищенность информации могут оказать действия персонала, что влечет за собой снижение эффективности защиты при любых других благоприятных условиях. Кроме этого в программном обеспечении могут возникать непреднамеренные ошибки и другие сбои информационной системы. Все это негативно влияет на эффективность защиты информации любого вида информационной безопасности, который существует и используется в информационных системах.

Защита информации от компьютерных вирусов предполагает программно-аппаратные средства защиты информации, которые предотвращают несанкционированное действие вредоносных программ, пытающихся завладеть данными и выслать их злоумышленнику, либо уничтожить информацию базы данных.

Задача защиты информации заключается в том, чтобы усложнить или сделать невозможным проникновение к данным, ради чего взломщики в своих противоправных действиях ищут наиболее достоверный источник секретных данных. А так как хакеры пытаются получить максимум достоверных секретных данных с минимальными затратами, то задачи защиты информации — стремление запутать злоумышленника: служба защиты информации предоставляет ему неверные данные, защита компьютерной информации пытается максимально изолировать базу данных от внешнего несанкционированного вмешательства.

Защита компьютерной информации для взломщика — это те мероприятия по защите информации, которые необходимо обойти для получения доступа к сведениям. Архитектура защиты компьютерной информации строится таким образом, чтобы злоумышленник столкнулся с множеством уровней защиты информации: защита сервера посредством разграничения доступа и системы аутентификации пользователей и защита компьютера самого пользователя, который работает с секретными данными. Защита компьютера и защита сервера одновременно позволяют организовать схему защиты компьютерной информации таким образом, чтобы взломщику было невозможно проникнуть в систему, пользуясь столь ненадежным средством защиты информации в сети, как человеческий фактор. То есть, даже обходя защиту компьютера пользователя базы данных и переходя на другой уровень защиты информации, хакер должен будет правильно воспользоваться данной привилегией, иначе защита сервера отклонит любые его запросы на получение данных и попытка обойти защиту компьютерной информации окажется тщетной.

Сегодня для реализации эффективного мероприятия по защите информации требуется не только разработка средства защиты информации в сети и разработка механизмов модели защиты информации, а реализация системного подхода или комплекса защиты информации — это комплекс взаимосвязанных мер. Данный комплекс, как правило, использует специальные технические и программные средства для организации мероприятий защиты информации. Однако нельзя исключать и человеческий фактор, что также необходимо предусматривать при защите информации.

Кроме того, сегодня разработаны и имеют место некоторые модели защиты информации, которые содержат нормативно-правовые акты и морально-этические меры защиты информации и противодействия атакам извне, что необходимо совершенствовать и дополнять с развитием научно-технического прогресса.