УДК 007

ИНФОРМАЦИОННАЯ БЕЗОПАСНОСТЬ КАК ЧАСТЬ СОВРЕМЕННОГО ОБЩЕСТВА

А.Н. РЫКОВ

Белорусский государственный университет информатики и радиоэлектроники
ул. П. Бровки, 6, г. Минск, 220013, Республика Беларусь
antonme66@mail.ru

Появление в мире новых рисков, вызовов и угроз, обострение глобальных проблем человечества, проблемы безопасности в политической сфере, насущные потребности по сохранению дальнейшего устойчивого развития Беларуси объективно потребовали поиска новых подходов к комплексному обеспечению национальной безопасности страны. [1]

Ключевые слова: информационная безопасность, информационные технологии, защита.

В сложившейся ситуации одним из важнейших направлений развития информационных технологий в современном обществе является информационная безопасность. В настоящее время в ее функции входит защита таких категорий информации, как научная, коммерческая и стратегическая [1].

Под понятием безопасности автоматизированной информационной системы понимают ее защищенность от преднамеренного и случайного вмешательства в нормальный процесс ее функционирования, а также от попыток модифицировать или разрушить ее компоненты. Это обеспечивает комплекс технологических и административных мер, которые применяются к программам, данным и аппаратным средствам с целью обеспечить доступность, целостность и конфиденциальность защищаемых ресурсов. В табл. 1 приведена систематизация ресурсов защиты информации.

Табл. 1. Основные ресурсы защиты информационной системы

Компьютерная безопасность	Совокупность технологических и административных мер, обеспечивающая доступность, целостность и конфиденциальность ресурсов компьютера
Безопасность данных	Защита данных от несанкционированной модификации, разрушения и раскрытия этих данных.
Безопасность коммуникаций	Предотвращение предоставления неавторизованным лицам информации, которая может быть выдана системой в ответ на запрос по каналам связи.
Безопасность программного обеспечения	Программное обеспечение, которое обеспечивает безопасную обработку данных в компьютерной системе, а также дает возможность безопасно использовать ресурсы системы.

Проблемой информационной безопасности начали заниматься, как только появилась угроза раскрытия засекреченной информации. Первым шагом стало распространение знаний об информационной безопасности за пределами правительственных организаций, непосредственно связанных с секретной информацией или отвечающих за режим секретности. Первый опубликованный материал – «Критерии оценки надежных компьютерных систем» («Оранжевая книга») увидела свет в США в 1983 году благодаря Министерству обороны США.

Согласно «Оранжевой книге» безопасной системой называется та система, которая «управляет посредством соответствующих средств доступом к информации, так что только должным образом авторизованные лица или процессы, действующие от их имени, получают право читать, записывать и удалять информацию». Очевидно, что абсо-

лютно безопасных систем не существует – каждую систему можно «взломать», если иметь достаточное количество времени и материальных ресурсов [1].

Надежная система – «система, использующая достаточные аппаратные и программные средства, чтобы обеспечить одновременную обработку информации разной степени секретности группой пользователей без нарушения прав доступа».

Сейчас крупные фирмы, банки, организации стараются защитить свою информацию от злоумышленников. Шпионская программа или программа способная разрушить целостность системы может быть замаскирована в любой файл. Стоить заметить, что не существует абсолютно безопасных систем. Каждую систему можно «взломать» если иметь достаточное количество временных и материальных ресурсов.

Для защиты информации существуют программы способные обнаруживать вероятные источники угроз и устранять их (так называемые антивирусы) или защищать информацию другими способами (шифрование, архивирование, или назначение пароля). Антивирусы способны отслеживать абсолютное большинство всех угроз и предотвращать атаки, то есть антивирус объединяет в себе черты средств активной защиты. Шифрование и введение паролей – элементы пассивной защиты информации (они не дают получить доступ к информации). Эти программы не допускают к работе с информацией неавторизованных пользователей или программы, действующие от их лица. Однако справится с такими программами намного легче, чем справится с пользователем, допустившим для системы фатальную ошибку. После него трудно восстановить систему и его почти невозможно обнаружить, если не иметь возможности протоколировать действия пользователей, так или иначе влияющих на безопасность системы. Однако протоколирование будет бесполезно без своевременного и грамотного анализа.

Представляется возможным предотвращение потери информации в хранении ее небольшими частями на разных носителях и в разных местах. Это избавит систему от возможных ошибок, атак или проблем с носителями информации. Подобная система сейчас активно применяется в авиатехнике. Также возможны случаи, когда злоумышленникам удастся собрать все части, тогда необходимо позаботится о безопасности информации. Для таких случаев эти части кодируются. Если все части закодированы одинаково, то безопасность кода значительно уменьшается. Однако если каждую часть кодировать по своему, то весь объем информации будет слишком велик и труднообрабатываем.

Существует множество способов защиты информации, лучший результат они дают при их совмещении. Для каждой угрозы существует своя защита и при правильном использовании они выполняют свои функции. В итоге сам пользователь решает, каким образом защищать важную для него информацию и прибегает к различным методам.

Список литературы

1. Информационно-аналитический центр при Администрации Президента Республики Беларусь: Информационный материал № 6 (90). Обеспечение национальной безопасности Республики Беларусь как важнейший фактор развития государства в современных условиях. [Электронный ресурс]. – Режим доступа: http://iac.gov.by/nfiles/000046_480473.pdf. – Дата доступа: 08.04.12.