Николай НИКОЛОВ, аспирант

Хозяйственная Академия им. Д.А.Ценова (Свиштов, Болгария)

УГРОЗЫ ИНФОРМАЦИОННОЙ БЕЗОПАСНОСТИ

Информационная безопасность организационных систем управления подразумевает обеспечение целостности, конфиденциальности и доступности данных.

Целостность означает, что данные не были модифицированы, заменены или уничтожены в результате случайных или преднамеренных действий. Конфиденциальность данных – содержание критической информации в секрете, доступ к которой ограничен узким кругом пользователей, или свойство защищенности информации от несанкционированного доступа и попыток ее раскрытия пользователями, не имеющими соответствующих полномочий. Существует перечень данных, которые должны быть отнесены к конфиденциальным. К их числу относят такие, как личная информация пользователей, учетные записи (имена и пароли), данные о кредитных картах, различные внутренние документы, а также данные бухгалтерского учета.

Доступность данных означает получение возможности ознакомления с ней, ее обработка, в частности копирование, модификация или уничтожение.

обытие, которое может вызвать нарушение функционирования информационной системы, включая искажение, уничтожение или несанкционированное использование информации, называется угрозой. В специальной литературе используются разные классификации угроз. Существуют классы угроз информационной безопасности, которые можно условно объединить в следующие группы:

- непреднамеренные или случайные действия, выражающиеся в неадекватной поддержке механизмов защиты и ошибками в управлении;
- преднамеренные угрозы – несанкционированное получение информации и несанкционированная манипуляция данными, ресурсами и самими системами.

В свою очередь, преднамеренные угрозы объединяют следующие действия:

- физические, к которым относят хищения, уничтожение собственности, террористические акции и другие чрезвычайные обстоятельства;
- технические, к которым относят перехват информации, искажение, уничтожение и ввод ложной информации;
- интеллектуальные – уклонение от обязательств, мошенничество, скрытое наблюдение, психологическое воздействие.

В настоящее время основными угрозами принято считать следующие:

- ошибки в программном обеспечении. Системное и прикладное программное обеспечение содержит ошибки, поскольку оно написано людьми, а людям свойственно ошибаться. Наличие ошибок приводит к появлению уязвимостей, которые могут быть использованы злоумышленниками для получения несанкционированного доступа к ресурсам информационной системы, получения контроля над серверами и др. Подобные ошибки устраняются с помощью пакетов обновлений, выпускаемых производителями программного обеспечения и своевременная установка таких пакетов является необходимым условием политики безопасности;
- отказы в обслуживании и распределенные атаки. Они направлены на выведение сети или сервера из работоспособного состояния. Их реализация приводит к перегрузке сетевого канала трафиком и его блокировке;
- программные злоупотребления. К ним относят сетевые компьютерные вирусы, троянские кони и др. Основой их функционирования являются уязвимости в используемом программном обеспечении, а основными средствами распространения – электронная почта;
- анализаторы протоколов и снифферы. К данной группе относят аппаратные и программные средства перехвата информации, используемые злоумышленниками;
- технические средства съема информации. К данной группе относят клавиатурные шпионы, устройства записи звука и видеоизображения.

Отдельную группу образуют угрозы, порождаемые «человеческим фактором». К ним относят такие, как уволенные или недовольные сотрудники, промышленный шпионаж, халатность и низкая квалификация персонала.

Литература:

1. Батурин Ю.М., Жиджитский А.М. Компьютерная преступность и компьютерная безопасность. – М.: Юридическая литература, 1991.
2. Герасименко В.А. Защита информации в автоматизированных системах обработки данных. – М.: Энергоатомиздат, 1994.
3. Панасенко С.П., Батура В.П Основы криптографии для экономистов. – М.: Финансы и статистика, 2005.