АНАЛИЗ УГРОЗ ИНФОРМАЦИОННОЙ БЕЗОПАСНОСТИ

А.В. Корвель
Научный руководитель – В.Ф. Алексеев
канд.техн.наук, доцент
Белорусский государственный университет информатики и радиоэлектроники

Под угрозой безопасности объекта будем понимать потенциально существующую возможность случайного или преднамеренного действия, или, без действия, в результате которого может быть нарушена его безопасность.

Основным средством реализации угрозы является несанкционированный доступ (НСД) субъекта к объекту.

Угрозы безопасности можно классифицировать по различным признакам: по цели воздействия, по типу воздействия, по типу источника, по месту источника и др. [1-4]. Можно указать следующие основные виды угроз.

По цели воздействия можно выделить следующие типы угроз: нарушения конфиденциальности; нарушения целостности; нарушения работоспособности; раскрытия параметров системы.

Угрозы нарушения конфиденциальности (секретности) направлены на получении доступа к объектам (информации, имуществу) лицам, которые не должны иметь к ней доступ. Это происходит при несанкционированном доступе к некоторым закрытым объектам, который не связан с непосредственным их изменением или повреждением.

Если система обеспечения защиты перестает нормально функционировать, то возможно осуществление запрещенного доступа. Каналы утечки характеризуют ту ситуацию, которую проектировщики не сумели предусмотреть. Поэтому система не в состоянии рассматривать такой доступ как запрещенный. Утрата контроля за защитой может возникнуть в критической ситуации, которая может быть создана стихийно или искусственно.

Каналы утечки информации могут быть нескольких видов: каналы утечки по памяти (образуются за счет использования доступа к общим объектам системы); каналы утечки по времени (является каналом, передающим противнику информацию о процессе, промоделированном ценной за крытой информацией).

Нарушением целостности информации или имущества является незаконное их изменение или искажение, приводящее к нарушению ее качества или полному уничтожению. Это имеет место и при воздействии на имущество, напри мер, кража его.

Традиционно защита целостности относится к категории организационных мер. К уничтожению и модификации могут привести случайные и

преднамеренные критические ситуации в системе, вирусы, «троянские кони» и т.д. Защита целостности имущества выполняется за счет ограничения доступа к нему. Используются также механизмы устойчивости к ошибкам, защита от вирусов и защита от нарушений доступности.

Угрозы нарушения работоспособности направлены на создание таких ситуаций, при которых снижается производительность работы, защищаемой организации или ее систем, блокируются возможности выполнения отдельных функций или доступ к некоторым ресурсам. К этому типу угроз следует отнести угрозы нарушения работоспособности самой системы безопасности. Нарушение работоспособности могут быть постоянными или временными.

Угрозы раскрытия параметров системы (структуры организации, план помещений, данные о системе безопасности) не причиняют непосредственно ущерб имуществу или информации, но способствуют возможности реализации угроз других видов. Это характеризует угрозы разведки параметров системы.

По типу воздействия угрозы безопасности можно разделить на случайные и преднамеренные.

Причинами случайных воздействий могут быть: аварийные ситуации вследствие стихийных бедствий, аварий или отключения электропитания; отказы, сбои и помехи в аппаратуре; ошибки разработчиков аппаратуры и программного обеспечения ошибки обслуживающего персонала, операторов и пользователей; ошибки в линиях связи.

Преднамеренные угрозы связаны с целенаправленными действиями нарушителя. Преднамеренные угрозы могут быть осуществлены «взломщиками из вне, посетителями организации и служащими данной организации (превышение полномочий). Примерами таких угроз могут быть: ознакомление легальных пользователей системы с закрытой для них информацией; проникновение на закрытую территорию посторонних лиц; несанкционированное копирование программ, данных и документов; несанкционированная умышленная модификация информации, про-грамм, документов, баз данных; несанкционированное изменение, модификация или блокирование работы различных технических систем; фальсификация сообщений, передаваемых по каналам связи, отказ от авторства сообщений или факта получения сообщений; умышленное уничтожение программ, данных и имущества. кража имущества, документов и носителей информации.

Автором исследуется защита от преднамеренных угроз. По типу источника преднамеренные угрозы могут быть разделены на: угроза непосредственного воздействия; угроза удаленного воздействия.

Угроза непосредственного воздействия имеет место, когда нарушитель имеет непосредственный физический доступ к некоторому объекту и возможность оказать на него воздействие. Примером таких действий является вывод из строя аппаратуры, порча имущества, несанкционированное копирование документации и т.п.

Такая угроза возникает при условии получения злоумышленником непосредственного физического доступа к защищаемым объектам.

Угроза удаленного воздействия осуществляется без непосредственного контакта с объектом атаки. Это может быть несанкционированное

копирование информации через компьютерную сеть, блокирование работы некоторых систем путем занесения неверной управляющей информации и т.п. Такое воздействие может выполняться через компьютерную сеть (чаще всего) или электрическую сеть (обесточивание).

По месту источника преднамеренные угрозы могут быть разделены на непосредственная угроза объекту на месте его размещения: удаленная угроза с компьютеров, подключенных к сети; удаленная угроза с территории, на которой развернута система; перехват и модификация информации, передаваемой по каналам связи.

Вне зависимости от источника и вида угроз система безопасности должна обеспечивать следующие свойства защищаемых объектов: конфиденциальность, целостность, доступность.

Из изложенного краткого рассмотрения угроз безопасности объектов можно сделать вывод, что для надежной защиты организации от угроз необходимо ограничивать как физический, так и удаленный доступ к объектам защищаемой организации. Для защиты самой системы безопасности в сетевой среде необходимо защищать ее аппаратные средства, данные и линии передачи информации. Это подтверждает представленную аксиому о решающей роли контроля над доступом субъектов к объектам в вопросах обеспечения безопасности.

Библиографический список

1. Korchenko A., Prystavka P, Kazmirchuk S., Akhmetov B. Analytical verification expressions of linguistic variables for information security risk assessment systems // Ukrainian Scientific Journal of Information Security, 2017, vol. 23, issue 1, p. 50-55.

2. Корченко А.Г. Построение систем защиты информации на нечетких множествах. Теория и практические решения К.: МК-ПресС, 2006. — 320 с.

3. Зегжда Д. П. Основы безопасности информационных систем : Учебное пособие для вузов по специальности "Компьютерная безопасность" и "Комплексное обеспечение информационной безопасности автоматизированных систем " / Д. П. Зегжда, А. М. Ивашко . – М. : Горячая Линия-Телеком, 2000 . – 452 с.

4. Малюк А.А. Информационная безопасность. Концептуальные и методологические основы защиты информации 2004. – 280 с.