АНОНИМНОСТЬ, КАК КОМПОНЕНТ СИСТЕМЫ ЗАЩИТЫ ИНФОРМАЦИИ ПРИ ИСПОЛЬЗОВАНИИ КОМПЬЮТЕРНЫХ СЕТЕЙ

А.Л. Мастыкин

Подавляющее большинство посетителей сети «Интернет» входят в нее открыто (не пытаясь скрыть связь виртуальной личности и физического лица). Даже при деятельности пользователя не меняющей структуры данных в сети, при открытом входе в нее, сервисы сети считывают пользовательские данные, позволяющие организовать атаку, для получения более ценной информации о пользователе и файловой системы его компьютера или гаджета. Обеспечение безопасности данных пользователя сети интернет является комплексной задачей, выполнение которой немыслимо без реализации анонимности.

Вариантом решения проблемы может служить:

– использование специальных пакетов программ для достижения скрытой работы в сети;

– настройка используемого программного обеспечения, к примеру, запрет (в настройках браузера) на cookie и java script;

– применение основного принципа анонимности, не оставлять реальных данных о себе, в том числе, и в социальных сетях;

– использование фиктивных виртуальных личностей, и их распределенное применение (для посещения отдельного ресурса – специальная личность, которую сложно связать с любой другой личностью на ином ресурсе);

– применение строгой модели поведения в сети, исключающей деанонимизацию личности;

– удаление логов на рабочей машине о своем пребывании в сети;

– использование приватных ключей шифрования и хранения их в месте доступном лишь обладателю.

АДАПТИВНЫЙ ПОДХОД К СИСТЕМЕ ЗАЩИТЫ ИНФОРМАЦИИ

Д.Ю. Недосеко

В настоящее время непрерывно совершенствуются процессы защиты информации.

В соответствии с теорией защиты информации существует два подхода к построению системы защиты: фрагментарный и системный [1]. Фрагментарный подход направлен на противодействие четко определенным угрозам. В качестве примеров реализации подхода можно указать отдельные средства управления доступом, автономные средства шифрования, специализированные антивирусные программы и т.д. Достоинством данного подхода является высокая избирательность к конкретной угрозе. Существенные недостатки – отсутствие единой защищенной среды обработки информации, потеря эффективности защиты при видоизменении угрозы безопасности, внешней среды, деятельности организации. Фрагментарный подход к защите информации применяется только в узких рамках и лишь для обеспечения безопасности относительно простых КИС. В современных же условиях наиболее рациональным и правильным является использование системного подхода к защите информации. Системный подход ориентирован на создание защищенной среды обработки информации, объединяющей в единую систему средства противодействия угрозам. Организация защищенной среды позволяет гарантировать определенный уровень безопасности КИС, что является несомненным достоинством системного подхода. Недостатки подхода — ограничение на свободу действий пользователей системы, большая чувствительность к ошибкам установки и настройки средств защиты, сложности управления. Как правило, системный подход применяют для защиты КИС крупных организаций или небольших систем, выполняющих ответственные задачи или обрабатывающих особо важную информацию.

Библиотека БГУИР