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

С учетом достоинств и недостатков вышеприведенных подходов предлагается адаптивный подход к системе защиты информации. Обращая внимание на необходимость исполнения должностных обязанностей (в зависимости от занимаемой должности), а также учитывая навыки работы с ПК (низкий, средний, высокий, профессиональный) возможно ограничение доступа к информации — с разрешением только на чтение, модификацию, копирование либо удаление. Стоит обратить особое внимание при внезапном изменении поведения сотрудника и ограничить доступ к возможности модификации либо удаления информации в такой ситуации. Более подробно об этом будет рассмотрено в ходе выступления.

Литература

1. *Леонов А.П.* Безопасность автоматизированных банковских и офисных систем. Минск, 1996.

ПОЛИТИКИ БЕЗОПАСНОСТИ КАК СОСТАВНАЯ ЧАСТЬ КОМПЛЕКСНОЙ ЗАЩИТЫ ИНФОРМАЦИИ ПРЕДПРИЯТИЯ

Р.В. Паршукова, А.М. Прудник

Производственные, технологические, коммерческие данные, которые используют предприятия, обладают высокой стоимостью, а их утрата или утечка может привести к серьезным финансовым потерям. Поэтому одной из целей для предприятий отрасли является создание надежной системы защиты информации.

Система защиты информации — это комплекс организационных и технических мер, направленных на обеспечение информационной безопасности предприятия. Главным объектом защиты являются данные, которые обрабатываются в автоматизированной системе управления и задействованы при выполнении бизнес-процессов [1].

Процесс создания системы защиты информации можно разделить на три этапа:

– формирование политики предприятия в области информационной безопасности;

– выбор и внедрение технических и программных средств защиты;

– разработка и проведение ряда организационных мероприятий.

Фундаментом для создания системы защиты информации является документ, в котором формулируются принципы и основные положения политики предприятия в области информационной безопасности.

Политика информационной безопасности определяет стратегию и тактику построения корпоративной системы защиты информации. Политика безопасности компании является основой для разработки целого ряда документов безопасности: стандартов, руководств, процедур, практик, регламентов, должностных инструкций и прочее другое [2].

Общий жизненный цикл политики информационной безопасности включает в себя ряд основных шагов:

– проведение предварительного исследования состояния информационной безопасности;

– разработку политики безопасности;

– внедрение разработанных политик безопасности.

Политика безопасности затрагивает практически каждого сотрудника компании. Опыт создания политик безопасности показывает, что внедрение политики безопасности часто приводит к возникновению напряженности во взаимоотношениях между сотрудниками компании. Если это возможно, о том, что разрабатывается новая политика информационной безопасности компании необходимо уведомить сотрудников заранее. До начала внедрения новой политики безопасности желательно предоставить сотрудникам текст политики на одну–две недели для ознакомления и внесения поправок и комментариев. Политика безопасности должна быть реалистичной и выполнимой, быть краткой и понятной, а также не приводить к существенному снижению общей производительности бизнес подразделений компании. Политика безопасности должна содержать основные цели и задачи организации

Библиотека БГУИР