УДК 004.725.7

ОЦЕНКА УЩЕРБА ОТ ВОЗДЕЙСТВИЯ КОМПЬЮТЕРНЫХ АТАК НА ТЕРРИТОРИАЛЬНО-РАСПРЕДЕЛЕННЫЕ СЕТИ, ИСПОЛЬЗУЮЩИЕ ЗАЩИЩЕННЫЕ МОБИЛЬНЫЕ АВТОМАТИЗИРОВАННЫЕ РАБОЧИЕ МЕСТА

Д.А. Алексеев

Рассматривается процесс обеспечения безопасности мобильных автоматизированных рабочих мест (МАРМ), входящих в автоматизированную систему государственного управления, и методический подход к оценке возможного экономического ущерба от компьютерных атак.

Ключевые слова: мобильные автоматизированные рабочие места, оценка финансовых убытков.

Сложнейшая задача, которая решается сегодня в России, – это создание «электронного правительства», посредством которого будет обеспечен доступ к государственным услугам максимального количества отечественных и зарубежных пользователей через сеть Интернет в режиме реального времени (on-line). Важнейшими инструментами обеспечения взаимодействия госструктур с пользователями являются действующая автоматизированная система государственного управления (АСГУ) и многообразие типов электронных устройств, стационарных и мобильных, к которым относятся ноутбуки, миникомпьютеры, коммуникаторы, флэш-устройства, iPad, мобильные телефоны и другие носители информации. Условно эти мобильные средства можно назвать МАРМ, в том числе и те, которые входят в состав АСГУ. Схематично АСГУ представляет собой структуру, организованную по территориально-распределенному принципу и состоящую из множества случайных пользователей, способных в режиме on-line вести с ней обмен данных через центральный сервер в установленном порядке. Организация такого взаимодействия сопровождается серьезным противоречием: необходимостью открытого доступа к АСГУ, с одной стороны, и наличием системы защиты информации от подключаемых к ней пользователей, которые могут нанести ущерб ее функционированию, с другой стороны.

Процесс обеспечения безопасности МАРМ, входящих в АСГУ, должен включать следующие основные этапы оценки рисков компьютерных атак: информационный аудит, определение степени внедряемой безопасности, обучение пользователей. Целями управления рисками являются: выявление угроз, измерение, контроль и минимизация потерь, связанных с неопределенными негативными событиями или рисками. Оценка риска включает в себя такие задачи, как анализ угроз, выбор приоритетов, выявление уязвимостей и определение типов рисков, поиск путей сокращения потерь, а также принятие решения в отношении снижения угрозы или исключения риска [1, 2]. Кроме того, управление рисками в информационных сетях является дорогостоящей проблемой, так как после успешной компьютерной атаки затраты на восстановление сетей могут быть несоизмеримо большими по сравнению с ее созданием. Так, военные США уже в 2010 г. потратили более $ 100 млн. на восстановление сетей и программного обеспечения после компьютерных атак [3].

В методике оценки ущерба предлагается учитывать прямые и косвенные потери при нарушении работоспособности информационной системы [1, 3]. Прямые (основные) потери от атаки на АСГУ будут включать нарушение процессов управления и принятия решений. Косвенный (побочный) ущерб характеризуется несвоевременностью, ошибочностью принятия или непринятием управленческого решения. Если нарушен процесс принятия решений в области международных отношений и (или) в военной сфере, то косвенные потери будут выражены как краткосрочными, так и долгосрочными последствиями в виде утраты стратегического управления государственной системы.

При оценке ущерба принимается во внимание, что в случае линейного возрастания последствия атаки, сумма косвенных или нематериальных потерь может увеличиваться нелинейно. Тогда общее увеличение стоимости потерь при высоких скоростях, масштабах и сложностях атак может расти по экспоненциальной зависимости. В тщательно спроектированных сложных информационных территориально-распределенных системах отказоустойчивость может предотвратить некоторые катастрофические последствия несанкционированного воздействия. Тем не менее, компьютерные атаки на информационные системы, даже самые защищенные, могут привести к экономическим потерям.

Такой методический подход может быть взят за основу при разработке модели кибербезопасности, позволяющей прогнозировать реакцию системы на атаку до ее реализации, используя понятия риска, уязвимости системы, времени между атаками и вторжениями (их количество и продолжительность).

1. Климов С.М. Методы и модели противодействия компьютерным атакам. – Люберцы: КАТАЛИТ, 2008.
2. Graham J.H., Ralston P.S. Quantitatively assessing the vulnerability of critical information systems: A new method for evaluating security enhancements // International Journal of Information Management. – 2008. – 28(6).
3. CBS News. Pentagon Bill to Fix Cyber Attacks: $100M. 2009 [Электронный ресурс]. – Режим доступа: http://www.cbsnews.com/, своб.

Алексеев Дмитрий Александрович – Санкт-Петербургский государственный университет информационных технологий, механик и оптики, аспирант, dima99@gmail.com