Методы защиты конфиденциальной информации в Интернете

Президент России Владимир Путин подписал указ о создании государственной системы обнаружения, предупреждения и ликвидации последствий компьютерных атак на информационные ресурсы, системы и ИКТ-сети, находящиеся на территории страны, а также в дипломатических представительствах и консульских учреждениях России за рубежом.

Как следует из опубликованного документа, основными задачами антихакерской системы должны стать прогнозирование ситуаций в области обеспечения информационной безопасности, поддержка взаимодействия владельцев информационных ресурсов с операторами связи и другими организациями, осуществляющими деятельность в области защиты информации, при решении задач, связанных с обнаружением и ликвидацией компьютерных атак. Система должна осуществлять контроль степени защищенности критической информационной инфраструктуры от компьютерных атак и устанавливать причины подобных инцидентов.

Организовать работы по созданию системы, разработать методические рекомендации по организации защиты и определить порядок обмена информацией между федеральными органами власти России и международными организациями Владимир Путин поручил ФСБ.

В настоящее время готовится целый ряд нормативных документов, которые должны конкретизировать задачу по созданию новой системы.

Реализацией основной части работ займутся Центр информационной безопасности и Центр защиты информации ФСБ.

В настоящее время антихакерская работа построена следующим образом: «Центр информационной безопасности идентифицирует атаку и сообщает о ней в Центр защиты информации, который, в свою очередь, занимается ее детальным изучением и расследованием».

Хакеры стали реальной силой, угрожающей безопасности не только отдельных компаний, но и финансовой и государственной инфраструктуре в целом.

Создание комплексной системы, оперирующей актуальными знаниями и навыками в области методов хакинга, – это единственный способ эффективно противостоять киберпреступникам.

Интересно, что указ президент подписал на следующий день после того, как в суд были переданы материалы уголовного дела в отношении 30-летнего жителя Красноярска, обвиняемого в атаке на сайт президента. 6 и 7 мая 2012 г., из-за атаки портал kremlin.ru был недоступен в течение часа.

В связи с этим дело было возбуждено по статье «Создание, использование и распространение вредоносных компьютерных программ», предполагающей наказание до четырех лет лишения свободы.

Предупрежден, но не защищен

14 февраля в московском офисе Академии информационных систем (АИС) прошел открытый семинар «Методы защиты конфиденциальной информации от действий инсайдеров, рейдерства и мошенничества. Приемы конкурентной разведки в Интернете», в котором приняли участие около 30 слушателей из числа руководителей служб информационной безопасности и ИТ-отделов, а также специалисты по маркетингу и менеджеры по продажам.

Семинар провел авторитетный эксперт по конкурентной разведке и тренер академии Андрей Масалович *(ил. 1)*.

ил. 1

По его словам, поиск в Интернете привычными поисковыми системами (Yandex, Google и пр.) дает пользователям возможность «добраться» только до 10 % информации, размещенной в Сети.

Для эффективной работы в Интернете и получения необходимой, подчас закрытой, информации, по методике Масаловича, нужно изменить в первую очередь подход к процессу поиска.

Он продемонстрировал на реальных примерах методы работы сотрудников служб безопасности и наглядно показал, что такое «невидимый» Ин-


ил. 2

тернет, объяснил, почему и как «утекает» конфиденциальная информация в глобальную Сеть *(ил. 2)*.

«Моя многолетняя практика показывает, что знание принципов конкурентной разведки в Интернете и практическое применение специальных поисковых машин необходимы в работе любого руководителя компании, начальника отдела информационных технологий (от англ. information technology, IT) и начальника отдела информационной безопасности, маркетолога или специалиста по продажам и работе с клиентами», – считает Андрей Масалович. – Причем умения и знания в области конкурентной разведки одинаково важны для любой отрасли. На нашем семинаре были представители и банковской сферы, и крупных интернет-компаний, авиаперевозчиков, телеком-сектора и промышленности» *(ил. 3)*.

Большую часть семинара Андрей Масалович посвятил демонстрации использования аналитических технологий и наступательных методов информационной безопасности в реальных задачах конфиденциальной информации.

Слушатели оставили много положительных отзывов о проведенном мероприятии, заметив, что с интересом прослушали бы полный курс по теме *(ил. 4)*.

Академия информационных систем имеет лицензию Департамента образования г. Москвы на право ведения образовательной деятельности по направлению «Конкурентная разведка в Интернете».

Материал подготовлен совместно с пресс-службой НОУ «АИС»

Фото ИПК «ИнтерКрим-пресс»

<<<<< СПРАВКА

Институт непрерывности бизнеса (BCI, Би-Си-Ай) совместно с Британским институтом стандартов (BST, Би-Эс-Ай) опубликовал результаты исследования, согласно которым 65 % компаний обеспокоены или чрезвычайно обеспокоены возможностью интернет-атак в 2013 г.

Также исследование показало, что 71 % респондентов считают использование сети Интернет для хакерских атак важной тенденцией, с которой необходимо справиться с помощью стратегии непрерывности бизнеса. 42 % из них стараются управлять рисками, связанными с доминированием широко распространенных зависящих от Интернета сервисов.

В исследовании участвовали 730 компаний из широкого круга областей (финансовые услуги, государственная служба и безопасность, торговля и производство) из 62 стран, включая США, Великобританию, Индию, Китай, Южную Африку, Египет и Бразилию.

Также в отчете по исследованию, которое проводится уже два года подряд, содержится следующая информация:

В 2013 г. основной угрозой, которая вызывает опасения, стали незапланированные отключения Интернета и связи. 70 % компаний заявили, что они обеспокоены или чрезвычайно обеспокоены данной угрозой в 2013 г. За ней идет угроза утечки данных, которая вызывает опасения у 66 % респондентов.

Отмечаются стабильные темпы инвестирования в непрерывность бизнеса, несмотря на экономический кризис. 22 % респондентов увеличат инвестиции в 2013 г., и 54 % заявили, что будут их поддерживать на приемлемом уровне. 14 % респондентов предполагают сократить инвестиции, что ограничит область применения или снизит результативность программы.


ил. 3

ил. 4