panorama2002№10март.

# По мнению специалистов, многие компании недооценивают масштабы угрозы информационной безопасности.

12 марта в отеле Hyatt Regency состоялся семинар "Корпоративные системы безопасности", организованный Ernst&Young, Actis Systems Asia и "Лабораторией Касперского". Этот альянс всемирно известной консалтинговой компании с популярным российским разработчиком антивирусов и отечественным лидером e-business-услуг необычен лишь на первый взгляд. Ernst&Young уже более 10 лет активно занимается вопросами информационной безопасности.

"Лаборатория Касперского" с нынешнего года отказалась от присутствия в своем логотипе слова "антивирус", заменив его на "безопасность". Заместитель директора по корпоративным решениям "Лаборатории Касперского" Рустэм ХАЙРЕТДИНОВ объяснил этот шаг следующим образом. Компании чаще страдают от вирусов, чем от хакеров. Но ущерб от хакеров несравнимо больше. Соответственно, информационная безопасность не может ограничиваться разработкой только компьютерных антивирусов.

Проблеме хакерства (кибертерроризма) или несанкционированных компьютерных проникновений большое внимание в своем докладе уделила руководитель группы по оказанию услуг в области информационных технологий и ИТ-рисков в СНГ компании Ernst&Young Мишель МУР. По ее словам, в мире сейчас помимо "шалящих" время от времени студентов и школьников насчитывается порядка 19 млн хакеров экстра-класса. Г-н Хайретдинов считает, что часть из них, вероятно, являются бывшими или действующими разработчиками систем информационной безопасности. Что касается самой техники электронного взлома, то, по данным г-на Хайретдинова, для грамотного хакера подбор паролей (наиболее распространенная система защиты) не представляет проблемы. 80% паролей подбираются в течение первого часа работы, 10% - за сутки, и лишь 10% (в виде сложных сочетаний) принципиально недешифруемы.

Говоря об источниках угрозы информбезопасности, г-жа Мур назвала в числе таковых несколько внешних и внутренних: это может быть как конкурент, так и случайный хакер; человек, желающий свести личные счеты (например, уволенный или чем-то недовольный сотрудник), а также наивный сотрудник, случайно "взломавший" сеть. По данным г-жи Мур, основанным на результатах специально проведенного в прошлом году исследования, 80% рисков исходят из внутренних источников и лишь 20% - из внешних. Однако одной из главных причин роста кибертерроризма она считает недооценку фактора угрозы информационной безопасности самой компанией, ее руководством. Многие компании, особенно в СНГ, наивно полагают, что они неизвестны, скупятся на наем специалистов и покупку защитных программ. А значит, являются идеальными объектами для атак хакеров.

Примечательно, что из 110 опрошенных Ernst&Young крупных компаний 60% так или иначе страдали от хакеров и вирусов. При этом большинство (более 70%) пострадавших компаний, как правило, ничего не предпринимают, так как чаще всего даже не знают, что делать.

Между тем, по данным г-на Хайретдинова, вместе с ростом электронного бизнеса увеличивается общий ущерб от кибертерроризма. Так, если в 1999 году компьютерные вирусы нанесли убытки в размере $6,1 млрд, то в прошлом - уже $13,2 млрд. Абсолютным "хитом" стал при этом вирус "LoveBug", известный больше как "I love you". Ущерб от этого саморассылающегося вируса составил в 2000 году $8,75 млрд. Именно из-за него 2000 год стал рекордным в плане вирус-убытков ($17,1 млрд). Собственно, благодаря вирусам и хакерам рынок технологий по информационной безопасности тоже растет очень интенсивно - на 70% в год.

Г-н Хайретдинов при этом согласился с резонностью расхожего мнения о том, что вирусы вполне могут создаваться разработчиками антивирусных программ. Однако, по его мнению, такой путь слишком примитивен и опасен, так как конкуренция на рынке очень высока. Соответственно, очень важна репутация и высока вероятность того, что грамотные конкуренты смогут всегда доказать твою причастность. Собственно, эти два фактора являются гарантией соблюдения правил на ИТ-рынке.

Технически информационная безопасность сейчас обеспечивается целой системой мер. Причем, по словам г-на Хайретдинова, это должно быть комплексное решение, включающее фильтрацию данных, контроль доступа, crypto (шифрование), обучение специалистов, сервисное обслуживание и др.

Генеральный директор Actis Systems Asia Константин КАРДЫМОН кратко описал казахстанский рынок информационных технологий. По его словам, объем его в 2001 году составил $85 млн. Важным моментом г-н Кардымон считает новую правительственную программу формирования и развития национальной информационной инфраструктуры на 2001-2003 гг. Однако при этом глава Actis Systems Asia констатирует отсутствие четкого подхода к решению проблем защиты информации в нашей стране. Причины этого он видит в недостаточной информированности ИТ-специалистов о проблеме и возможностях ее решения, неразвитой законодательной базе, необъективном представлении некоторых руководителей о существующей угрозе бизнес-процессам.

По словам г-на Кардымона, в основном только руководители крупных финансовых организаций считают защиту информации важной статьей расходов, разрабатывают собственные или используют созданные специально для них системы безопасности (как физическая защита, так и информационная). В остальных же случаях вся защита сводится к примитивным антивирусным системам и охране у входа в здание.
Другими причинами недостаточного внимания к информационной защите были названы относительно невысокая стоимость секьюрити-систем и низкая конкуренция на рынке по сравнению с Западом.

Адиль ДЖАЛИЛОВ.