РАЗДЕЛ I

ИНФОРМАЦИОННЫЕ ТЕХНОЛОГИИ В УПРАВЛЕНИИ И БИЗНЕСЕ

Н. А. Бабина
Киевский национальный университет
технологий и дизайна, г. Киев, Украина

«ИНФОРМАЦИОГЕННАЯ» СОСТАВЛЯЮЩАЯ ЭКОНОМИЧЕСКОЙ БЕЗОПАСНОСТИ ПРЕДПРИЯТИЯ

Преступления в сфере информационных технологий включают как распространение вредоносных вирусов, взлом паролей, кражу номеров кредитных карточек и других банковских реквизитов (фишинг), так и распространение противоправной информации (клеветы, материалов порнографического характера, материалов, возбуждающих межнациональную и межрелигиозную вражду и т. п.) через Интернет, коммунальные объекты. Кроме того, одним из наиболее опасных и распространенных преступлений, совершаемых с использованием Интернета, является мошенничество. В зарубежных государствах, в частности в США, получили распространение аферы, связанные с продажей доменных имен.

В соответствии с действующим уголовным законодательством Российской Федерации под преступлениями в сфере компьютерной информации понимаются совершаемые в сфере информационных процессов и посягающие на информационную безопасность деяния, предметом которых являются информация и компьютерные средства[1].

Одним из видов компьютерной преступности можно считать компьютерное пиратство (пиратство в сфере использования информационных технологий). По данным исследовательской компании IDC, уровень компьютерного пиратства на Украине составляет 83 %. Это значит, что на 83 % из 15 млн работающих в стране компьютеров установлена хоть одна нелегальная копия какого-либо программного

[1] *Преступления* в сфере информационных технологий // Википедия: свободная энциклопедия. URL: http://ru.wikipedia.org/wiki/Преступления_в_сфере_информационных_технологий

обеспечения. В основном это продукты компании Microsoft – Windows и Office, компании Adobe – Photoshop, Illustrator и PageMaker, а также других производителей (например, игр)[1].

По оценкам специалистов Microsoft, средний уровень электронного пиратства в Центральной и Восточной Европе (32 страны) составляет 70 %. Для определения уровня пиратства мы обращаемся к нескольким организациям и ассоциациям в данной отрасли (BSA, IDC). Здесь нужно отметить, что они изучают уровень пиратства, скорее, среди предприятий, а не среди потребителей. Это и малые предприятия, и очень крупные, включая госсектор. В таких отраслях экономики Украины, как телекоммуникации, банковский и финансовый сектор, страховые компании, уровень пиратства достаточно низок. Самый высокий уровень пиратства – в сфере малого бизнеса.

Одной из причин распространения пиратства называют высокую цену продуктов. Однако довольно объектов становятся дешевые продукты, например, в игровой индустрии.

У пиратства много причин, и не только ценовых. Их нужно рассматривать в комплексе. Главное – чтобы чиновники, бизнесмены и обычные пользователи начали понимать, что такое право интеллектуальной собственности.

Microsoft стала одним из двигателей борьбы с компьютерным пиратством на Украине и в России. Компания инициировала программу льготной легализации программного обеспечения в школах и государственных учреждениях. Была создана рабочая группа по легализации и правам интеллектуальной собственности. Однако реальных результатов почти нет.

Разрабатывается методология оценки информационных технологий для того или иного предприятия. Условно говоря, на крайней левой позиции этой шкалы предприятие рассматривает программное обеспечение как инструмент своей деятельности, с которым связаны затраты. Крайняя правая позиция – организация рассматривает информационные технологии как свой стратегический актив, составляющий часть ее капитала. В течение жизненного цикла каждая организация перемещается от крайней левой позиции к крайней правой[2].

Сейчас в России зарегистрировано около 35 млн активных пользователей Интернета, на Украине – почти 10 млн, постоянно увеличивается и количество пользователей ПК. Индустрия высоких

---

[1] http://www.idc.com/

[2] *Дашян М. С.* Право информационных магистралей (Law of information highways): вопросы правового регулирования в сфере Интернет. М.: Волтерс Клувер, 2007.

технологий растет на 40 % в год. Рынок становится зрелым. Эксперты высказывают мнение, что российская и украинская экономики не слишком подвержены основным угрозам информационной безопасности – вирусным и хакерским атакам, краже персональных данных, потому что уровень развития высоких технологий в этих экономиках достаточно низкий.

Во многих странах возникают серьезные скандалы, когда взламываются базы данных кредитных карт, похищается другая приватная информация или коммерческие секреты попадают в руки конкурентов. Есть также вопросы безопасности детей в Интернете. Правительство должно озаботиться информационной безопасностью государства в целом и граждан в частности.

Жизнь каждой страны зависит от киберсистем, которые на сегодняшний день чрезвычайно уязвимы для атак, в том числе террористических. В то же время, многие из этих систем достаточно просты, т. е. очень уязвимы. Возможны атаки на телекоммуникации, Интернет, мобильные системы связи. В мире нет страны, которая была бы защищена от компьютерных атак. Специфика кибератак состоит в том, что их можно организовать легко и дешево – достаточно лишь нескольких инженеров.

Не исключено, что в будущем конфликты между государствами и организациями перейдут в киберпространство. В будущем кибератаки станут агрессивнее и будут проводиться с целью не только заработка или шпионажа, но и демонстрации силы атакующих. Кроме того, увеличится количество угроз для пользователей мобильных и облачных технологий, а также для аудитории социальных сетей.

Мобильное рекламное ПО (madware, mobile advertising software) может не только сильно помешать процессу использования устройства, но и выдать злоумышленникам детали местоположения владельца, контактные данные, а также идентификационные данные устройства. Программа типа madware, незаметно попадающая на устройство при установке стороннего приложения, часто начинает заваливать пользователя всплывающими окнами, создает ярлыки, меняет настройки браузера и собирает личные данные.

Специалисты отмечают, что пользователи с большим доверием относятся к социальным сетям, начиная от обмена личными данными и заканчивая покупкой игровой валюты и виртуальных подарков друзьям. По мере того как с целью повышения уровня монетизации социальные сети предоставляют пользователям возможность дарить друг другу настоящие подарки, рост денежного оборота в социаль-

ных сетях дает злоумышленникам новые возможности для осуществления атак.

Эксперты ожидают роста числа атак, направленных на кражу платежных данных в социальных сетях и обман пользователей с целью заставить их сообщить эти и другие данные поддельным соцсетям. Сюда могут входить фальшивые извещения о подарках и электронные письма, требующие от пользователя указать свой домашний адрес и иную личную информацию. И хотя предоставление нефинансовой информации может показаться делом безобидным, злоумышленники торгуют и обмениваются ей, объединяя данные с уже имеющимися, что зачастую позволяет им получать доступ к по-настоящему ценной информации.

Кроме того, включение в корпоративные сети незащищенных устройств, собирающих информацию, которая после этого оседает на других облачных носителях, значительно повышает риск утечки или целенаправленного захвата данных. Установка пользователями все новых приложений в конечном счете неизбежно приводит к заражению.

Некоторые вредоносные мобильные программы дублируют функционал уже существовавших угроз, например тех, что крадут информацию с устройств. Однако иногда появляется и что-то новое. Например, во времена dial-up-модемов существовали программы, которые звонили на 900 номеров, принадлежащих хакерам. Сегодня вредоносные программы отправляют платные СМС-сообщения, и вырученные средства достаются злоумышленникам. В будущем можно будет наблюдать дальнейшее развитие мобильных технологий, что создаст новые возможности для киберпреступников.

Набирающая популярность технология электронных кошельков eWallet неизбежно станет еще одной платформой, которую злоумышленники попытаются использовать в своих целях. А по мере повсеместного внедрения технологий мобильных платежей мобильные устройства станут представлять еще большую ценность. По аналогии с угрозой Firesheep для перехвата чужих Wi-Fi-сессий стоит ожидать появления программ, которые будут перехватывать платежную информацию пользователей. Некоторые платежные системы популярны среди технически неискушенных пользователей и могут быть уязвимы, что потенциально приведет к краже информации.