



*Голубев В. А.*

*кандидат юридических наук, доцент  
профессор кафедры уголовного права и  
правосудия юридического факультета  
Запорожского национального университета*

## КИБЕРПРЕСТУПНОСТЬ - НОВЫЕ УГРОЗЫ

Подобно многим революционным технологиям, глобальная сеть Internet предоставляет огромные возможности как для прогресса, так и для злоупотреблений. Атаки в сети, мошенничества с пластиковыми платежными карточками, кражи средств из банковских счетов, корпоративный шпионаж, распространение детской порнографии - это лишь некоторые из преступлений, которые дубятся в сети Internet. Такие противоправные деяния составляют для нашего государства, как и для многих других стран мира, значительную общественную опасность, реально угрожая информационной безопасности - составляющей национальной безопасности.

Национальная инфраструктура государства уже сегодня тесно связана с использованием современных компьютерных технологий. Ежедневная деятельность банковских и энергетических систем, управления воздушным движением, транспортная сеть, даже скорая медицинская помощь находятся в полной зависимости от надежной и безопасной работы автоматизированных электронно-вычислительных систем.

Преступность в сфере использования компьютерных технологий ("киберпреступность") - это явление международного значения,

уровень которого непосредственно зависит от уровня развития и внедрения современных компьютерных технологий, сетей их общего пользования и доступа к ним. Таким образом, стремительное развитие информатизации в Украине несет в себе потенциальную возможность использования компьютерных технологий из корыстных и других мотивов, что в известной мере ставит под угрозу национальную безопасность государства.

Основной целью киберпреступника является компьютерная система, которая управляет разнообразными процессами, та информация, что циркулирует в них. В отличие от обычного преступника, что действует в реальном мире, киберпреступник не использует традиционное оружие - нож и пистолет. Его арсенал - информационное оружие, все инструменты, которые используются для проникновения у сети, взлома и модификации программного обеспечения, несанкционированного получения информации или блокировки работы компьютерных систем. К оружию киберпреступника можно прибавить компьютерные вирусы, программные закладки, разнообразные виды атак, которые делают возможным несанкционированный доступ к компьютерной системе. В арсенале

современных компьютерных преступников есть не только традиционные средства, но и самое современное информационное оружие и оборудование; эта проблема уже давно пересекла границы государств и получила международное значение.

Вместе с последующим внедрением современных информационных технологий в Украине постоянно растет угроза как для государственных компьютерных систем, так и для частных организаций и отдельных граждан.

Особенную актуальность проблема киберпреступности приобрела в наше время. Социологические опросы в разных странах, и в первую очередь в высокоразвитых, показывают, что киберпреступность занимает одно из главных мест среди тех проблем, которые тревожат людей. Более того, по мнению специалистов, сегодня это явление составляет значительно более серьезную опасность, чем 5 лет назад, в связи с использованием преступниками новейших информационных технологий, а также через растущую уязвимость современного индустриального общества. Независимо от усилий государств, которые направлены на борьбу с киберпреступниками, их количество в мире не уменьшается, а, напротив, постоянно растет.

Ни одно государство сегодня не способно противостоять этому злу самостоятельно. Неотложной является потребность активизации международного сотрудничества, для которого является актуальным, в частности, налаживание международно-правового механизма регулирования. Но, ввиду того, что в современных условиях значительная часть средств борьбы с киберпреступлениями, как и с другими преступлениями международного характера, принадлежит к внутренней компетенции каждого отдельного государства, необходимо параллельно развивать и национальное законодательство, направленное на борьбу с компьютерными преступлениями, согласо-

вывая его с международными нормами права и опираясь на существующий позитивный опыт.

Отсутствие эффективных механизмов борьбы с киберпреступлениями определяется сегодня как одна из угроз национальной безопасности нашего государства. При таких обстоятельствах Украина, как независимое демократическое государство, не может стоять в стороне от проблем противодействия компьютерной преступности и, в частности, ее транснациональных (трансграничных) форм.

Рассмотрим типичные категории компьютерных преступлений и те негативные последствия, с которыми общество сталкивается уже сегодня.

Инсайдеры (Insiders) - лица, которые имеют доступ к внутренней информации. Чаще всего именно они негативно настроены против своих работодателей. Инсайдер (работающий или освобожденный сотрудник компании) является потенциальным преступником. Знакомый с тонкостями компьютерной системы компании, он имеет неограниченный доступ к системе с целью незаконного вмешательства в работу автоматизированных электронно-вычислительных машин, их систем или компьютерных сетей или с целью незаконного завладеет информацией, которая является собственностью компании.

Как пример, можно привести случай, когда Национальная библиотека медицинской литературы (National Library of Medicine - NLM) к которой обращаются сотни тысяч практикующих врачей и специалистов в отрасли медицины из всего мира для получения информации о заболевании, лечении, медикаментах, испытала нападение со стороны инсайдера. Тот осуществил несанкционированный доступ к главной системе защиты информации, загрузив сотни файлов, в том числе наиболее важные - категории "скорая помощь", и файлы программного обеспечения, от которых зависела бесперебойная работа системы. Эти нарушения привели к значительным

негативным последствиям в работе всей системы и убытков в размере 25 тыс. долларов. Расследование, проведенное ФБР США, установило лицо преступника, которым оказался Монтгомери Джон Грей (Montgomery Johns Gray) - программист, чей доступ в компьютерную систему был аннулирован компанией после его освобождения. Он совершил взлом через "черный вход", созданный им же в программном коде. Преступник был арестован ФБР как носителя угрозы обществу

Хакеры (Hackers) также составляют большую опасность. Иногда они взламывают сети просто ради острых ощущений или ради завоевания авторитета в хакерских кругах. Но нередко это происходит с целью финансовой наживы и других злодеяний. Как правило, хакеры - прекрасные знатоки информационной техники, которые имеют неординарные способности, поэтому для них не является проблемой манипулирование компьютерными системами на расстоянии: они не санкционировано перекачивают тексты и протоколы с World Wide Web на сайты компьютера жертвы. Преступления, когда происходит блокировка обслуживания (DDOS - атака), - еще одно доказательство того, что экономический саботаж полностью возможен при использовании надлежащих и доступных программных инструментов в сети Internet.

В последнее время участились политически мотивированные атаки на вебсайты и серверы электронной почты, которые за приемами выполнения дублируют "хакерство". В таких случаях группа или отдельные субъекты перегружают серверы электронной почты или стирают вебсайты для передачи политических сообщений. Хотя такие виды нарушений не приводят к повреждению операционных систем или сети, однако они становятся причиной сбоев работы электронной почты, что в свою очередь приводит к большим денежным расходам и блокировки доступа абонентов к вебсайтам,

на которых находится ценная информация. Да, в 1996 году был совершен несанкционированный доступ к компьютерной системе вебсайта Министерства юстиции США. Злоумышленники уничтожили содержание свыше 200 каталогов и разместили страницы с изображением Адольфа Гитлера, свастики, сцен порнографического характера и тому подобное.

В Украине ежегодно раскрывается около 500 преступлений в сфере использования компьютерных технологий.

В 2007 году наиболее распространенными преступлениями были мошенничество с использованием компьютерной техники, несанкционированный сбыт и распространение информации с ограниченным доступом, несанкционированное вмешательство в работу компьютерных и телекоммуникационных систем, подделки банковских платежных карточек, а также мошенничество со стороны операторов связи и абонентов телекоммуникационных компаний.

Служба безопасности Украины только за первый месяц 2007 года возбудила 15 уголовных дел за преступления в сфере компьютерных технологий. В частности, представителями СБУ были задержаны продавцы информации с ограниченным доступом, базами телефонной сети 09, ГАИ МВД Украины, налоговой администрации, таможни.

В России в прошлом году было зафиксировано около 14 тысяч компьютерных преступлений. Чрезвычайно разнообразны компьютерные мошенничества: это ложные предложения товаров и услуг через Интернет, услуги по организации хакерских атак, аферы с электронными платежными картами и счетами клиентов электронных платежных систем. В прошлом году было пресечено свыше 450 таких преступлений. Статистика показывает, что почти в 43% случаев жертвами компьютерных мошенников становятся участники онлайн-аукционов - когда покупатель кликает на недобросовестное

предложение приобрести какой-нибудь товар по очень низкой цене, но с предоплатой.

Особую обеспокоенность вызывает безопасность Интернет. Необходимость привлечения внимания к проблеме безопасности в Сети вызвана тем, что виртуальная среда давно сравнялась по опасности с реальной. Неприятности, приходящие из компьютера, примерно те же, что и в обычной жизни: вирусы, кражи и грабежи, хамство и преследование, вымогательства и угрозы, незтичная и навязчивая реклама, терроризм и экстремизм. Украденные хакерами деньги уже давно считаются миллиардами, а к некоторым вирусам по несколько месяцев не могут подобрать противоядие. "Отморозки" всех рангов и званий назначают свои встречи через Сеть, там же отдают приказы об "акциях" и отчитываются об их исполнении (от очередного побитого "инородца" до взорванного дома). Таким образом, Всемирная сеть, идеальный источник информации и развлечений, может стать для любого из нас и идеальным источником проблем.

Статистика говорит сама за себя:

- ◆ 86% атакуемых хакерами компьютеров - домашние;
- ◆ Спам составляет 54% контролируемого трафика электронной почты в мире, в России - 82% трафика;
- ◆ Рост фишинговых (связанных с сетевым мошенничеством) сообщений на июль 2006 года составил 81%;
- ◆ 18% обезвреженных образцов вредоносных вирусов - новые;
- ◆ 4,2 млн. сайтов - порнографические;
- ◆ 55% блоггеров пишут свои Интернет-дневники под псевдонимом, опасаясь негативных последствий в реальной жизни;

Пожалуй, наиболее уязвимыми для потока информационного мусора из Всемирной

сети являются дети. Исследования показали, что 90% детей сталкивались в Интернете с порнографией, а 65% искали ее целенаправленно. Интерес к "клубничке" привел к тому что 44% несовершеннолетних пользователей Интернет хотя бы раз подвергались сексуальным домогательствам в Сети. Эти данные не покажутся столь удивительными, если иметь в виду что половина детей выходит в Интернет без всякого контроля со стороны родителей или педагогов. Более того, как показывают опросы, большинство из них настолько доверчивы, что готовы предоставить "виртуальному другу" в Интернете свои личные данные (вплоть до пин-кодов кредиток родителей).

После того, как были созданы 217 тыс программ, нацеленных на нанесение ущерба персональным компьютерам, мир организованной преступности осознал потенциальный выгоды от операций в киберпространстве и теперь сосредоточил усилия на похищении личных данных пользователей, отмечается в докладе "Десять основных угроз безопасности в 2007 году", подготовленном экспертами "МакАфи".

Проблема противодействия компьютерной преступности - это комплексная проблема. Сегодня законы должны соответствовать требованиям, предъявляемым современным уровнем развития технологий. С этой целью необходимо проводить целенаправленную работу по гармонизации и совершенствованию законодательства, регулирующих распространение информации в телекоммуникационных сетях. Одним из приоритетным направлением является также организация взаимодействия и координации усилий правоохранительных органов, спецслужб, судебной системы, обеспечение их необходимой материально-технической базой.