Могилевский институт МВД

УДК 341.4

О. И. Левшук
доцент кафедры административной деятельности ОВД факультета милиции Академии МВД Республики Беларусь, кандидат юридических наук, доцент

МИРОВОЙ ОПЫТ ПРОТИВОДЕЙСТВИЯ КИБЕРАТАКАМ

Сегодня масштабной проблемой мирового сообщества являются киберпреступления, численность которых ежегодно растет. Потенциальными жертвами преступных посягательств становятся как население, так и государственные (негосударственные) организации. Поэтому главной задачей любого государства является обеспечение информационной безопасности путем реализации мер, направленных на предотвращение несанкционированного проникновения в компьютерные системы, незаконного завладения компьютерной информацией в киберпространстве.

Под кибербезопасностью понимается прежде всего оперативное реагирование на угрозы внутри сети Интернет. В большинстве случаев объектами кибератак становятся Интернет вещей и промышленный Интернет вещей, так как, во-первых, невысока степень защиты устройств и портов, облачных приложений, интерфейсов программирования приложений; во-вторых, отсутствуют стандарты поддержания безопасности. Как правило, разработчики и подрядчики прежде всего обращают внимание на функциональность устройств, нежели на потенциальные риски и возможные последствия [1].

В 2017 году 200 тыс. организаций более чем в 150 странах стали жертвами вредоносных программ (вирусов WannaCry и Petya), целевое назначение которых сводилось к блокированию файлов на компьютерах для последующего вымогательства денег. Уже в 2019 году были осуществлены компьютерные взломы (несанкционированные доступы) — British Airways и Marriot Sherwood Hotels, Facebook, Google+ [2, с. 37]. Это повлекло вложение значительного количества инвестиций в разработку программных продуктов в сфере кибербезопасности, создание групп специалистов по защите компьютерных систем, которые пополнили штатную численность организаций.

В Великобритании с 2006 года образована некоммерческая организация CREST, ведающая вопросами информационной безопасности, за-

нимающаяся аккредитацией организаций и сертификацией физических лиц, оказывающих услуги в IT-сфере. Членами CREST являются компании, ежегодно проходящие аккредитацию. Высокие требования предъявляются и к частным лицам, желающим пройти сертификацию в CREST. Они сдают экзамены различной степени сложности (с учетом опыта работы), где должны продемонстрировать свои знания, умения и навыки в качестве высококвалифицированных специалистов в IT-сфере. Сертифицированные специалисты каждые три года пересдают экзамены.

Благодаря этой организации разработаны системы технической оценки и сертификации стандартов кибербезопасности для правительства Англии — Cyber Essentials и Cyber Essentials Plus, позволяющие защитить от вредоносных программ, в частности от вируса WannaCry. Главное — выработка мер защиты веб-сайтов, приложений, баз данных, серверов, компьютерных сетей, мобильных устройств (ноутбуков, портативных мини-компьютеров, мобильных телефонов и др.) и т. д. [2].

В 2019 году в Австралии создан центр кибернетического взаимодействия, целью функционирования которого является развитие компаний путем вывода новых товаров и услуг на мировые рынки. В качестве направлений его деятельности выделены: подготовка сотрудников IT-сферы всех уровней; проведение непосредственно организациями тестирований используемого оборудования и сетевых конфигураций на предмет безопасности и др. [3]. В качестве стратегических направлений борьбы с киберпреступностью правительством Австралии определены: подготовка специалистов для экстренного реагирования на кибератаки; формирование группы IT-экспертов для разработки и внедрения мер по укреплению кибербезопасности правительственных учреждений; введение в школах уроков интернет-безопасности [4].

Правительство Бразилии в 2018 году выработало стратегию в сфере информационной безопасности. В частности, в апреле 2018 года Национальный финансовый совет страны подготовил резолюцию, в которой было изложено требование о привлечении подрядчиков по обработке, хранению и использованию цифровой информации. В том же году был издан нормативный правовой акт «Общий закон о защите персональных данных», и с августа 2020 года начнет свою работу Национальный орган по защите информации. В настоящее время в Бразилии имеется Центр изучения, реагирования и устранения происшествий в компьютерной безопасности (CERT.br), специалисты которого реагируют на киберугрозы. При этом в качестве направления совершенствования дея-

тельности по защите компьютерной информации предлагается повысить уровень осведомленности общественности о проблемах кибербезопасности и создать горячую линию для жертв киберпреступлений [5].

В КНР также активно ведется борьба с киберпреступностью. Уголовный кодекс КНР с 1997 года дополнялся новыми статьями, предусматривающими ответственность за компьютерные преступления. С июня 2017 года действует Закон о кибербезопасности Китайской Народной Республики, который регламентирует сбор, хранение, обработку пользовательских данных, определяет обязанности участников системы информационной безопасности, предусматривает наказание за их нарушение или невыполнение.

Проведенные исследования киберпреступлений, жертвами которых стали жители Китая, позволили выделить и обобщить эти общественно опасные деяния в следующие группы:

- кражи реальных активов в виде несанкционированного доступа к банковским или платежным онлайн-аккаунтам (отмывание денег происходит путем перевода средств на аккаунты преступника с вымышленными данными с последующим обналичиванием денег через банкоматы, либо похищенные активы используются для приобретения карточек магазинов или платежных карт);

- кражи виртуальных активов (после взлома аккаунта переводятся активы на другой аккаунт или меняются пароль и настройки аккаунта для обеспечения контроля над ним, а в последующем захваченные активы или аккаунты выставляются на продажу на черном рынке);

- взлом интернет-ресурсов;

- хакерские технологии (разработка и реализация вредоносных программ; подбор и обучение лиц киберпреступной деятельности [6, с. 36–37].

Несмотря на принимаемые меры противодействия указанным преступлениям со стороны правительства КНР, данное направление попрежнему остается актуальным. Отсутствие специалистов в области борьбы с киберпреступлениями; снисходительная позиция судей при назначении наказаний за данные общественно опасные деяния; неосведомленность населения о киберпреступности и ее вреде, а также о мерах защиты цифровой информации от преступных посягательств (наиболее уязвимыми объектами кибератак оказались компьютерные системы школ и медицинских учреждений) по сути создают условия для развития киберпреступности. Именно на их устранение, по мнению правительства КНР, должна быть направлена работа в сфере информаци-

онной безопасности. Одновременно при разработке эффективных мер по противодействию киберпреступлениям должны учитываться результаты мониторинга нерегулярных денежных потоков.

Распространенность киберпреступлений во всем мире обуславливает поиск новых подходов по обеспечению информационной безопасности и разработке мер по противодействию киберпреступности. Конечно же, никто не может обеспечить стопроцентную защищенность от кибератак. Однако, чтобы не стать жертвой таковых, надо сохранять данные в облаке, систематически менять пароли, прибегать к шифрованию и внедрению новых способов проверки подлинности (аутентификации). С учетом транснационального характера рассматриваемых преступлений именно тесное сотрудничество стран (государств) позволит своевременно предотвратить такие противоправные деяния, а соответственно, причинение имущественного ущерба физическим или юридическим лицам в результате кибератак.

Список основных источников

1. Тенденции в сфере кибербезопасности в 2019 году / пер. С. Велев // Борьба с преступностью за рубежом: по материалам иностр. печ. — 2019. — № 4. — С. 6–8. Вернуться к статье

2. Услуги по обеспечению кибербезопасности / пер. Е. Харитонова // Борьба с преступностью за рубежом: по материалам иностр. печ. — 2019. — № 9. — С. 37–40. Вернуться к статье

3. Новый центр по обеспечению кибербезопасности в Австралии / пер. С. Велев // Борьба с преступностью за рубежом: по материалам иностр. печ. — 2019. — № 10. — С. 9. Вернуться к статье

4. Австралия ставит заслон киберпреступности. Премьер-министр представил стратегию кибербезопасности [Электронный ресурс]. — Режим доступа: https:/www.kommersant/ru/doc/296960. — Дата доступа: 15.01.2020. Вернуться к статье

5. Вопросы кибербезопасности в Бразилии / пер. С. Велев // Борьба с преступностью за рубежом: по материалам иностр. печ. — 2019. — № 3. — С. 11–14. Вернуться к статье

6. Классификация киберпреступности в КНР на основе внесенных судебных решений / пер. Е. Харитонова // Борьба с преступностью за рубежом: по материалам иностр. печ. — 2019. — № 8. — С. 33–46. Вернуться к статье