Для обеспечения проведения указанных удаленных обследований необходимо предусмотреть возможность использования правоохранительными органами специализированного программного обеспечения, позволяющего осуществлять удаленный контроль за средствами компьютерной техники, используемыми для совершения преступлений, доступ к хранящимся на них данным и используемым удаленным сервисам (например, облачным ресурсам), а также дающего возможность отслеживать активность преступника в сети Интернет. Подобные меры, получившие неофициальное наименование «полицейский троян» уже давно предусмотрены в законодательстве и используются в практике деятельности полиции ряда государств мира [1, с. 130–134].

Список основных источников

1. Харевич, Д. Л. Негласное расследование в Германии : монография / Д. Л. Харевич ; М-во внутр. дел Респ. Беларусь, Акад. МВД. — Минск : Акад. МВД, 2010. — 287 с.

УДК 343.85(477)

А. В. Форос
профессор кафедры кибербезопасности
и информационного обеспечения
Одесского государственного университета внутренних дел,
кандидат юридических наук, доцент (Украина)

НЕКОТОРЫЕ АСПЕКТЫ ПРОТИВОДЕЙСТВИЯ КИБЕРПРЕСТУПНОСТИ В УКРАИНЕ

Проблема компьютерной преступности привлекла внимание сотрудников правоохранительных органов зарубежных стран с момента широкого внедрения компьютерных технологий, что вызвало целый ряд негативных последствий и обострение ситуации в сфере защиты информации и информационных технологий. Анализ международной практики свидетельствует о том, что за последние тридцать лет в числе выявленных корыстных преступлений широкое распространение получили именно компьютерные преступле-

ния. Массовый характер приобрели электронные хищения денежных средств в крупных и особо крупных размерах, причинение имущественного ущерба в сфере информационно-телекоммуникационных технологий, неправомерный доступ к охраняемой законом компьютерной информации, подделка электронных и обычных документов, распространение как незаконной, так и вредоносной информации, незаконная деятельность в сфере предоставления услуг, нарушение авторских прав и многие другие.

В последнее время в международной юридической практике широко используется термин «киберпреступность» — вид транснациональной преступной деятельности, базирующейся на использовании в качестве средств совершения преступлений киберпространства. Количество киберпреступлений неуклонно увеличивается, возрастает их удельный вес по размерам похищаемых сумм и другим видам ущерба в общей доле материальных потерь от обычных видов преступлений. Так, киберпреступность в Украине — это пятый по значимости вид экономической преступности после незаконного присвоения имущества, коррупции и взяточничества, недобросовестной конкуренции и манипуляций с финансовой отчетностью. По результатам исследований, на киберпреступность приходится 23 % случаев мошенничества в мире, и 17 % — в Украине. Согласно тем же данным, киберпреступления становятся все более сложными и изощренными, что значительно усложняет процесс их выявления и предупреждения. Это может привести к еще более значительным ущербам и потерям в будущем [1].

Международный опыт борьбы с преступностью свидетельствует о том, что одним из приоритетных направлений решения задачи эффективного противодействия современной преступной деятельности является активное использование правоохранительными органами различных мер профилактического характера. Предупредить киберпреступление намного легче и проще, чем его расследовать и раскрыть. Обычно выделяются три основные группы мер предупреждения киберпреступлений, составляющие в своей совокупности целостную систему противодействия этому социально опасному явлению: правовые, организационно-технические и криминалистические.

Выделить направления противодействия киберпреступности значительно сложнее в силу многогранности этого социального

явления. Отметим только два основных направления. К первому направлению следует отнести предупреждение киберпреступлений, предусматривающее создание, сертификацию, лицензирование и внедрение необходимых средств технической и программной защиты информации; создание специализированных организационных структур организаций и служб кибербезопасности, направленных на обеспечение надежного функционирования средств защиты, генерации ключей и паролей, контроль по их использованию, замене и уничтожению; подготовку квалифицированных кадров для правоохранительных органов.

Второе направление противодействия киберпреступности включает в себя выявление и предотвращение киберпреступлений. В стадии окончательного решения находится проблема организации эффективного взаимодействия и координации субъектов противодействия киберпреступности. Именно многогранность субъектов противодействия киберпреступности предусматривает многоуровневую координацию их деятельности.

Рассмотрим более детально систему субъектов противодействия киберпреступности в Украине. Так, с 1991 года при Генеральном секретариате Интерпола создается Рабочая группа по проблемам компьютерной преступности, уделяющая внимание вопросам международного сотрудничества при расследовании компьютерных преступлений. Как следствие, в Украине на базе НЦБ Интерпола создается Национальный центральный консультативный пункт по проблемам компьютерной преступности. Это позволило собрать и систематизировать материал о законодательном регулировании и организационном опыте борьбы с киберпреступностью в разных странах, подготовить ряд аналитических отчетов и публикаций по данной тематике, ознакомить сотрудников МВД, прокуратуры, суда с новым видом преступной деятельности и внести существенные изменения в уголовное законодательство страны. На протяжении последних пятнадцати лет в структурах СБУ и МВД создаются различные департаменты и отделы, основная задача которых заключается в борьбе с правонарушениями в сфере интеллектуальной собственности и высоких технологий, защиты информации и информационных ресурсов страны.

5 ноября 2015 года была создана новая Киберполиция, являющаяся структурным подразделением Национальной полиции Укра-

ины. Министр МВД Арсен Аваков указал: «Киберполиция — ваша защита в виртуальном пространстве и не только! Отныне, пользуясь Интернетом и его возможностями, вы сможете получать полицейскую помощь в режиме реального времени».

Таким образом, основная цель создания киберполиции заключается в реформировании и развитии подразделений МВД Украины, обеспечивающих подготовку и функционирование высококвалифицированных специалистов экспертных, оперативных и следственных подразделений полиции, осуществляющих борьбу с киберпреступностью и способных применять на высоком профессиональном уровне новейшие технологий в оперативно-служебной деятельности.

К основным задачам киберполиции относятся:

1. Реализация государственной политики в сфере борьбы с киберпреступностью.

2. Противодействие киберпреступлениям (осуществляется в различных сферах, а именно: в сфере использования платежных систем, в сфере электронной торговли и хозяйственной деятельности, в сфере интеллектуальной собственности, в сфере информационной безопасности).

3. Своевременное информирование общественности о появлении новых киберпреступлений.

4. Внедрение программных средств для систематизации и анализа информации о киберинцидентах, киберугрозах и киберпреступлениях.

5. Реагирование на запросы зарубежных партнеров, поступающие каналами Национальной круглосуточной сети контактных пунктов.

6. Участие в повышении квалификации сотрудников полиции в сфере применения компьютерных технологий в борьбе с преступностью.

7. Участие в международных операциях и взаимодействие в режиме реального времени. Обеспечение функционирования сети контактных пунктов между 90 странами мира.

Таким образом, мы можем сделать вывод, что противодействие киберпреступности заключается в трех основных направлениях деятельности: предупреждение киберпреступлений, общая организация борьбы с киберпреступностью и правоохранительная дея-

тельность, направленная именно на выявление, предотвращение и раскрытие киберпреступлений, применение мер уголовной ответственности и наказание лиц, совершивших киберпреступление. Предупреждение как одна из форм борьбы с преступностью предусматривает как общегосударственные мероприятия экономического, идеологического, правового и воспитательного характера, так и специальные — организационные, технические, программные и криптографические. Приоритетным направлением также является организация взаимодействия и координации усилий правоохранительных органов, спецслужб, судебной системы, обеспечение их необходимой материально-технической базой. На сегодняшний день ни одна страна не в состоянии противостоять киберпреступности самостоятельно, что обуславливает необходимость активизации международного сотрудничества в данной сфере.

Список основных источников

1. Украина. Всемирный обзор экономических преступлений [Электронный ресурс] // DocPlayer.ru. — Режим доступа: http://docplayer.ru/35182824-Ukraina-vsemirnyy-obzor-ekonomicheskih-prestupleniy.html. — Дата доступа: 11.10.2017.