УДК 343.7

Ю. С. Карчевская
старший инспектор отделения
по идеологической работе и кадровому обеспечению
исправительного учреждения
«Воспитательная колония № 2» (Беларусь)

КАРДИНГ КАК САМЫЙ ПОПУЛЯРНЫЙ ВИД КИБЕРПРЕСТУПНОСТИ НЕСОВЕРШЕННОЛЕТНИХ В РЕСПУБЛИКЕ БЕЛАРУСЬ

Развитие в Республике Беларусь, как и во всем мире, электронных технологий и коммуникационных сетей, всеобщая доступность в глобальной компьютерной сети Интернет различных информационных ресурсов способствовало появлению принципиально нового вида нарушения Закона — киберпреступности — незаконных действий, которые осуществляются людьми, использующими информационные технологии для преступных целей.

Мы рассмотрим в данной статье наиболее распространенный по статистическим данным на сегодняшний день вид киберпреступлений, совершаемых несовершеннолетними, — кардинг. Мошенничество с платежными картами, или кардинг (от англ. carding) — вид мошенничества, при котором производится операция с использованием платежной карты или ее реквизитов, не инициированная или не подтвержденная ее держателем. Для осуществления подобных операций несовершеннолетнему злоумышленнику нет необходимости иметь доступ к самой банковской карте — вполне достаточно знать ее реквизиты, такие, как номер, код CVV2/CVC2 или пин-код. Чужие деньги мошенник-кардер может перевести себе или же приобрести с их помощью какие-нибудь товары или услуги. Кардеры — именно так называют преступников, которые специализируются на банковских картах, — уже давно перестали быть в Беларуси редкостью.

В Республике Беларусь ежегодно отмечается рост данного вида преступлений. Общее увеличение количества киберпреступлений произошло в основном за счет статьи 212 Уголовного кодекса Республики Беларусь (далее — УК) («Хищение путем использования компьютерной техники»). В 2015 году по оконченным расследованием уголовным делам выявлено 38 несовершеннолетних, со-

вершивших хищения путем использования компьютерной техники. В 2016 году этот показатель увеличился до 48 лиц, соответственно, прирост составил 26 % к уровню 2016 года.

Самым распространенным примером, встречающимся в отношении преступлений, предусмотренных статьей 212 УК, является ввод несовершеннолетним преступником персонифицированного идентификационного номера (ПИН-кода) чужой пластиковой банковской карточки. К сожалению, часть вины порой лежит на самих владельцах: кто-то может оставить записанный пин-код рядом с картой или вообще записать секретные цифры на карточке. Существует также такой вид обмана, как «дружественное мошенничество», когда свободный доступ к карте имеют не всегда чистые на руку члены семьи, близкие друзья. Также еще преступление может совершаться путем подглядывания пин-кода из-за плеча с последующей кражей карты. Этот метод прост и весьма распространен.

Необходимо отметить, что согласно постановлению Национального банка Республики Беларусь № 843 с 05.08.2015 года в стране вводится принцип нулевой ответственности держателей банковских карточек. Это означает, что банки понесут официальную ответственность за деньги, украденные мошенниками с карточных счетов их клиентов. Если кража денег совершена по неосторожности владельца карты (например, он записал ПИН-код на самой карте либо передал ее третьем лицу), данный принцип не применяется.

На практике правоохранительные органы часто сталкиваются со случаями, когда начинающие кардеры ищут доступ к зарубежным карт-счетам. Найти необходимую информацию по карточкам сегодня не сложно. Дампы (реквизиты, открывающие доступ к деньгам на банковской карте) можно купить на различных кардерских веб-барахолках. Таким образом, подросток, сидя за компьютером в Беларуси, получает возможность оплачивать свои покупки в интернет-магазинах за счет граждан США или какой-либо европейской страны.

Еще одним видом хищения денежных средств с помощью банковской пластиковой карточки является изготовление фальшивых банкоматов. Данный способ является очень редким, так как требует определенной технической оснащенности: воры изготавливают фальшивые банкоматы, которые выглядят как настоящие, либо пе-

ределывают старые и размещают их в людных местах. Такой банкомат принимает карту, требует ввода секретного кода, после чего выдает сообщение о невозможности выдачи денег и возвращает карту [1, с. 35].

Также есть и весьма необычные методы хищения с использованием банковских карточек. Например, применение скиммеров. Это устройство, считывающее информацию с магнитных полос карт: считыватель вешается на щель для приема карты, а дополнительную клавиатуру накрывают настоящей. При пользовании «усовершенствованным» банкоматом считыватель сохраняет данные с вставляемых карт, а клавиатура — пин-коды. В результате украденных данных достаточно для того, чтобы изготовить дубликат карты и снять деньги со счета.

Большинство юных киберпреступников не задумываются о последствиях совершаемых преступных деяний. У таких подростков, как правило, завышенная самооценка: они считают себя неуловимыми. Плюс — чувство безнаказанности. Тем не менее правоохранители находят несовершеннолетних кардеров. Сколько по времени занимает этот процесс, зависит от разных факторов. Нередко подростки решаются на киберпреступление в результате попустительства взрослых.

За последние 10 лет в Республике Беларусь принималось немало серьезных мер по устранению причин и условий, способствующих совершению преступлений данного вида. С учетом указанных негативных тенденций уголовно-правовые нормы, касающиеся несовершеннолетних правонарушителей, постоянно совершенствуются, в том числе путем снижения возраста, с которого наступает уголовная ответственность. С 4 апреля 2016 года возраст лиц, подлежащих ответственности по статье 212 УК, снижен с 16 до 14 лет. Снижение возраста уголовной ответственности — исключительно превентивная мера. Она должна лишний раз заставить молодых людей задуматься о своем поведении, ведь тенденция такова, что киберпреступность в мире постоянно молодеет.

В предупреждении киберпреступлений подростков важное значение имеют активные меры ранней профилактики, то есть работа, направленная на предупреждение уголовно наказуемых деяний. Она может создать надежный социально-психологический заслон на пути к отрицательным импульсам и устремлениям в поведении под-

ростков, позволяя тем самым оперативно предупредить, пресечь возможность наступления тяжелых последствий.

Список основных источников

1. Хилюта, В. Орудие преступления — банковская пластиковая карточка... / В. Хилюта, Н. Сергейко // Юстиция Беларуси. — 2007. — № 4. — С. 35.

2. Национальный правовой Интернет-портал Республики Беларусь [Электронный ресурс]. — Режим доступа: http://mvd.gov.by/. — Дата доступа: 15.11.2017.

3. Национальный правовой Интернет-портал Республики Беларусь [Электронный ресурс]. — Режим доступа: http:// court.gov.by /. — Дата доступа: 15.11.2017.

4. Национальный Интернет-портал Республики Беларусь [Электронный ресурс]. — Режим доступа: http://pravo.by /. — Дата доступа: 17.11.2017.

5. Уголовный Кодекс Республики Беларусь [Электронный ресурс] : : 9 июля 1999 г., № 275-З : принят Палатой представителей 2 июня 1999 г. : одобр. Советом Респ. 24 июня 1999 г. : текст Кодекса по состоянию на 18 июля 2017 г. № 53-З // ЭТАЛОН. Законодательство Республики Беларусь / Нац. центр правовой информ. Респ. Беларусь. — Минск, 2017.

УДК 37+343.85(477)

О. В. Косаревская

доцент кафедры кибербезопасности
и информационного обеспечения
Одесского государственного университета внутренних дел,
кандидат педагогических наук, доцент (Украина)

ОСОБЕННОСТИ ИНФОРМАЦИОННО-ТЕХНОЛОГИЧЕСКОЙ ПОДГОТОВКИ БУДУЩИХ СПЕЦИАЛИСТОВ ПРАВООХРАНИТЕЛЬНОЙ ДЕЯТЕЛЬНОСТИ В СФЕРЕ БОРЬБЫ С КИБЕРПРЕСТУПНОСТЬЮ В ВУЗАХ УКРАИНЫ

Основными факторами стратегии в сфере высшего юридического образования в Украине выступают усовершенствование механизмов управления системы высшего юридического образова-