Изучение оперативно-розыскной практики подразделений по раскрытию преступлений в сфере высоких технологий Министерства внутренних дел Республики Беларусь, а также анализ уголовных дел, возбуждавшихся по ст. 212 Уголовного кодекса Республики Беларусь «Хищение путем использования компьютерной техники», позволили привести соответствующую классификацию после упорядочения и систематизации полученных сведений.

По мнению автора, все способы хищений, совершаемых с использованием компьютерной техники, могут быть разделены на две группы:

связанные с осуществлением прямого доступа к счету без нарушения системы защиты (совершаются лицами, имеющими в силу служебного положения такой доступ);

связанные с осуществлением опосредованного несанкционированного доступа к счету.

В свою очередь, во второй группе выделяются способы хищения:

неквалифицированные (характерные особенности: носят, как правило, случайный характер; преступник не имеет четкого плана по совершению преступного деяния, в том числе относительно завладения БПК или ее реквизитами, и дальнейшему распоряжению похищенным имуществом или сведениями);

квалифицированные (характерные особенности: чаще всего совершаются в составе организованных групп, участники которых могут быть незнакомы друг с другом; общение между участниками происходит посредством интернет-форумов, различных приложений, предназначенных для обмена сообщениями, с использованием возможностей шифрования каналов передачи данных; совершаются в соответствии с заранее разработанными схемами; участники выполняют определенные функции и решают конкретные задачи).

Квалифицированные способы делятся на:

реальный кардинг (основан на изготовлении дубликатов БПК с использованием специального оборудования);

вещевой кардинг (связан с целенаправленным неправомерным завладением реквизитами БПК, необходимыми для осуществления денежных переводов либо онлайн-платежей с целью последующего хищения имущества в различных предприятиях интернет-торговли);

хищения, основанные на использовании вредоносного программного обеспечения, позволяющего оказывать влияние на функционирование банковских технических средств.

Подводя итог, следует отметить, что высокие темпы информатизации в нашей стране оказали существенное влияние на стремительность эволюционных процессов в сфере хищений, совершаемых с использованием компьютерной техники. В течение относительно небольшого периода времени спектр таких преступлений значительно расширился в направлении от довольно простых и заурядных до высокотехнологичных. Выявленные тенденции предоставляют возможность сделать вывод о том, что приоритетное направление в сфере рассматриваемой противоправной деятельности заняли хищения, совершаемые с использованием реквизитов БПК. Этому способствовало удобство эксплуатации глобальной сети Интернет с практически безграничным числом возможностей, низкий уровень конкуренции, позволяющий людям с невысокой технической квалификацией получать существенные доходы по сравнению со средней в стране заработной платой, многообразие обучающей литературы и простота внедрения в преступную среду на условиях анонимности, а также беспечность людей во всем мире по отношению к своему имуществу и вопросам информационной безопасности.

УДК 355.4

О.О. Лемешевский

АКТУАЛЬНЫЕ ВОПРОСЫ ИНФОРМАЦИОННОЙ БЕЗОПАСНОСТИ НА ФАКУЛЬТЕТЕ ВНУТРЕННИХ ВОЙСК МВД РЕСПУБЛИКИ БЕЛАРУСЬ

В XXI веке – веке информации и новых, доселе неизвестных, технологий – трудно найти какую-либо область жизни общества, где бы ни использовались современные способы обработки и передачи информации. Однако подобные реалии не только развивают наше общество, но и создают условия, в немалой степени облегчающие осуществление преступных планов. Организованные преступные группы максимально используют возможности новых информационных технологий как для подготовки и совершения преступлений, так и для их сокрытия.

Еще 20–25 лет назад в Республике Беларусь этой проблемы, казалось, вообще не существовало. Не было ни самих киберпреступников, ни соответствующей законодательной базы. С приобретением независимости наша страна получила доступ к технологическим новшествам. Произошел своеобразный обмен: из бывшего СССР «утекали мозги», взамен наши знания обогащались тем бесценным высокотехнологическим опытом стран рыночной экономики, которого мы были лишены. Но к новым технологиям прилагался достаточно разнообразный «набор» совершенно новых, неизвестных ранее, преступлений. Кроме преступных деяний, где компьютерная техника была лишь средством или объектом преступления, появились совершенно специфические преступления, где объектом преступления стала информация, размещен-

ная и на персональных компьютерах, и на компьютерах, соединенных как в локальную, так и в глобальные информационные сети. Эти виды преступлений вошли в отдельный раздел Уголовного кодекса Республики Беларусь «Преступления против информационной безопасности».

Компьютерная преступность стала настоящим бичом экономики развитых государств. Так, например, 90 % фирм и организаций в Великобритании в разное время становились объектами электронного пиратства или находились под его угрозой, в Нидерландах жертвами компьютерной преступности стали 20 % различного рода предприятий. В ФРГ с использованием компьютеров ежегодно похищается 4 млрд евро, а во Франции – 1 млрд евро.

Наибольшую общественную опасность представляют преступления, связанные с неправомерным доступом к компьютерной информации. Известно, рассматриваемые правонарушения имеют очень высокую латентность, которая по различным данным составляет 85–90 %. Более того, факты обнаружения незаконного доступа к информационным ресурсам на 90 % носят случайный характер.

Анализ материалов отечественных уголовных дел позволяет сделать вывод о том, что основными причинами и условиями, способствующими совершению компьютерных преступлений, в большинстве случаев стали:

1) бесконтрольность за действиями обслуживающего персонала, что позволяет преступнику свободно использовать ЭВМ в качестве орудия совершения преступления;

2) низкий уровень программного обеспечения, которое не имеет контрольной защиты, обеспечивающей проверку соответствия и правильности вводимой информации;

3) несовершенство парольной системы защиты от несанкционированного доступа к рабочей станции и ее программному обеспечению, которая не обеспечивает достоверную идентификацию пользователя по индивидуальным биометрическим параметрам;

4) отсутствие должностного лица, отвечающего за режим секретности и конфиденциальности коммерческой информации;

5) отсутствие категорийности допуска сотрудников к документации строгой финансовой отчетности;

6) отсутствие договоров (контрактов) с сотрудниками на предмет неразглашения коммерческой и служебной тайны, персональных данных и иной конфиденциальной информации.

Для эффективной защиты от компьютерных преступлений и утечки служебной информации на факультете внутренних войск был выполнен ряд мероприятий:

1) просмотрена вся документация;

2) определены возможные каналы утечки информации;

3) ликвидированы слабые звенья в защите;

4) определены категории допуска для лиц, имеющих право доступа;

5) определена дисциплинарная ответственность за сохранность и санкционированность доступа к имеющимся информационным ресурсам;

6) организован периодический системный контроль качества защиты информации посредством проведения регламентных работ как самим лицом, ответственным за безопасность, так и с привлечением специалистов;

7) проведена классификация информации в соответствии с ее важностью;

8) определено должностное лицо, отвечающее за режим секретности и конфиденциальности информации;

9) обновлено защитное программное обеспечение.

Таким образом, на факультете внутренних войск на высоком уровне осуществляется защита и предупреждение утечек служебной информации, защита от возможности компьютерной преступности, совершенствование программного обеспечения.

УДК 343

В.Ю. Арчаков, О.С. Макаров

ПРАВОВЫЕ ПРОБЛЕМЫ ОБЕСПЕЧЕНИЯ ИНФОРМАЦИОННОЙ БЕЗОПАСНОСТИ В СОВРЕМЕННЫХ УСЛОВИЯХ

Заканчивается второе десятилетие XXI в. Наряду с такими вызовами человечеству, как потепление климата, истощение природных ресурсов, мы рассматриваем угрозы, вызванные глобальным процессом информатизации нашей цивилизации.

В связи с тем, что современное общество переместило свои социальные отношения в информационную среду, где традиционные, выработанные тысячелетиями регуляторы безопасности не действуют, а адекватные системы их защиты в информационной сфере пока не разработаны, социум претерпевает негативные последствия реализации информационных угроз: растет информационная преступность, на личность оказывается деструктивное информационное воздействие, развивается кризис тайн и т. д.

В обозначенных условиях рельефно проявляется дилемма: обозримый путь общественного развития пролегает через процессы информа-