8. Исследование алгоритмических и технологических особенностей новейших зарубежных и отечественных технических средств обработки информации.

9. Разработка методологии оценивания защищенности, комплексных методов и средств защиты технических средств обработки информации от физико-технических методов несанкционированного доступа, совершенствование соответствующей нормативной базы.

10. Сравнительный анализ тенденций развития физико-технических проблем защиты информации в стране и за рубежом.

11. Разработка и научное обоснование моделей угроз и стратегий защиты объектов от технических разведок.

12. Разработка методов и средств противодействия техническим разведкам с учетом эффективности функционирования.

13. Разработка методов и средств контроля состояния и достаточности принимаемых мер по противодействию техническим разведкам на объектах защиты.

Во-вторых, значимой для развития исследований в области технической защиты информации остается проблема хронического недофинансирования.

С целью минимизации пробелов в данном направлении, целесообразно разработать меры по стимулированию:

публикационной и патентной активности исследователей;

привлечения молодежи в исследовательскую деятельность;

привлечения бизнес-организациями молодых ученых к выполнению научных исследований в области информационной безопасности.

Одним из ключевых условий научного и технологического развития в области технической защиты информации должно стать участие крупных компаний. Поддержка научной деятельности – важнейший фактор сохранения коммерческой тайны и удержания сферы влияния на отечественном и мировом рынках. Кроме того, обеспечивается устойчивое финансирование научных организаций, которое позволяет формировать новые знания.

В-третьих, необходимо совершенствование кадровой политики в сфере технической защиты информации.

Существенное противодействие росту компьютерных преступлений может оказать грамотная политика в подборе и подготовке национальных кадров в сфере информационной безопасности.

Проведенные социологические исследования студентов и специалистов, работающих в области защиты информации, позволяют сделать следующие выводы:

1. Дерзость совершения компьютерных правонарушений у молодежи вызывает восхищение, желание самоутвердиться, показать себя с

лучшей стороны и привлечь к себе внимание. Среди других факторов, определяющих желание осуществлять компьютерные правонарушения, можно выделить желание заработать.

2. Многие абитуриенты, поступая на специальности, связанные с защитой информации, преследуют корыстную цель – научиться методам совершения компьютерных преступлений.

3. Подавляющее большинство студентов, обучающихся на специальностях, связанных с вычислительной техникой, очень слабо знают нормативные правовые документы по защите информации.

Анализ информации позволил выявить ряд условий, реализация которых даст возможность обеспечить качественную подготовку специалистов в области технической защиты информации.

Для выработки рекомендаций по совершенствованию подготовки специалистов в области технической защиты информации необходимо выделить три направления: учебно-воспитательное, учебно-методическое, организационно-административное.

Немаловажной задачей становится повышение квалификации специалистов в области защиты информации.

Приоритетным направлением должна быть подготовка кадров высшей научной квалификации, которые проводили бы исследования в области технической защиты информации.

УДК 343.985

А.А. Ковальчук

КЛАССИФИКАЦИЯ ХИЩЕНИЙ, СОВЕРШАЕМЫХ С ИСПОЛЬЗОВАНИЕМ КОМПЬЮТЕРНОЙ ТЕХНИКИ

В настоящее время жизнь людей буквально невообразима без привычных программно-технических средств, например компьютеров, которые позволяют автоматизировать сложнейшие процессы и существенно расширить человеческие возможности. Однако далеко не всегда достижения науки и техники используются во благо. Нередко отдельные представители общества, руководствуясь корыстными и иными деструктивными мотивами, совершают различного рода противоправные деяния.

На современном этапе широкое распространение получили хищения, совершаемые с использованием компьютерной техники. Впервые подобные преступления были выявлены на территории Республики Беларусь на рубеже прошлого и нынешнего веков и основывались на незаконном использовании банковских платежных карточек (БПК). В дальнейшем с развитием информационных технологий происходил процесс эволюции способов совершения хищений.

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-