ВЗГЛЯД НА ПРОБЛЕМУ ПРОФИЛАКТИКИ ПРЕСТУПЛЕНИЙ В СФЕРЕ ИНФОРМАЦИОННЫХ ТЕХНОЛОГИЙ

Яблонский Г.А. – начальник отдела по раскрытию преступлений в сфере высоких технологий УВД Витебского облисполкома

Возможность действовать быстро и анонимно в «цифровой среде», которая, как известно, не имеет реальных границ, сегодня являются определяющим фактором для повышения активности преступных сообществ, а увеличение темпов внедрения телекоммуникационной техники и информационных услуг, невольно вооружают криминальный элемент новыми возможностями для осуществления преступных замыслов.

Еще несколько лет назад авторитетная компания AppRiver провела исследования и установила, что вирусная активность в сети Интернет достигла своего пика. Количество единиц вредоносного программного обеспечения превышает 10 миллионов единиц в сутки.

В то время как в СМИ беспрерывно сообщается о хакерских атаках на web-ресурсы таких крупных компаний как Sony, Michael's of Chicago, Eidos Games, сеть телевидения Fox и многих других, западные специалисты по информационной безопасности отмечают, что на хакерских форумах наблюдалась небывалая активность по распространению программного обеспечения для создания вирусов.

Сегодня мировое интернет-сообщество полностью осознало тот факт, что стремительное развитие информационных технологий со-

провождается возникновением все новых угроз информационной безопасности. Активное внедрение инноваций в различные сферы нашей жизни создают значительную угрозу применения информационного оружия, как против индивидуальных, корпоративных информационных систем, так и против отдельно взятого государства в целом. В подобных условиях особое значение приобретают вопросы противодействия кибертерроризму и различным проявлениям экстремизма в сети Интернет.

В силу естественных процессов, связанных с быстрым инновационным развитием Республики Беларусь, вышеперечисленные проблемы все чаще становятся объективной реальностью для нашей страны. Естественный рост киберпреступлений происходит на фоне существенного ежегодного прироста числа абонентов сотовых сетей, новых компьютеров, подключаемых к сети Интернет, а также значительного увеличения объемов передаваемой информации.

Так, проникновение сотовой связи в стандарте GSM в республике уже давно перешагнуло отметку 100%.

Количество банковских платежных карточек, находящихся в обращении граждан, составляет более 12 миллионов единиц, в том числе свыше пяти миллионов карточек платежной системы «БЕЛКАРТ» и порядка семи миллионов – международных платежных систем.

В Республике Беларусь установлено более 3 600 инфокиосков, 4000 банкоматов, 52 000 организаций торговли (сервиса), где располагается свыше 76 000 платежных терминалов.

По данным Национального статистического комитета в Республике Беларусь по состоянию на начало т.г. насчитывалось более шести с половиной миллионов абонентов сети Интернет.

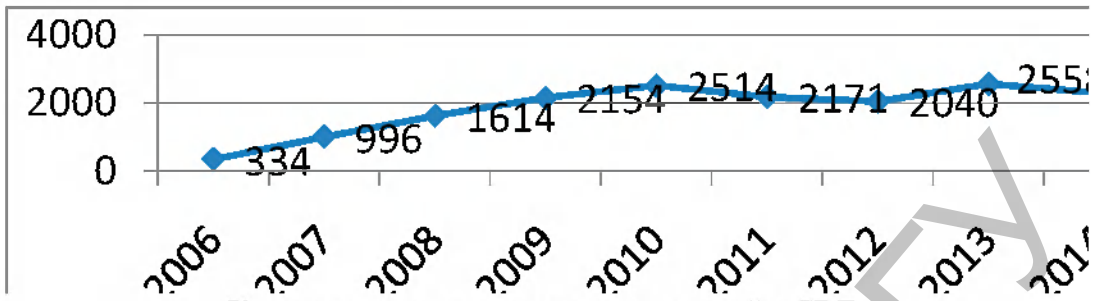
Больше всего пользователей интернета в возрастной группе 16–29 лет (66,2%), среди граждан 30–49 лет интернетчиков уже заметно меньше – 7,9%. В то же время все чаще попадают в поле зрения правоохранительных органов как несовершеннолетние, так и престарелые граждане нашей страны.

Следует иметь в виду, что официальная статистика не отражает реальное количество преступлений, относящихся к категории «кибер», в силу того, что последние высоко латентны. Объясняется это незнанием потерпевших о существовании ответственности за те или иные противоправные действия, совершенные в их отношении, а также нежеланием отдельных потерпевших сообщать о преступных посягательствах во избежание подрыва репутации, вследствие опасения наступления собственной ответственности, например за использование установленных на ПК контрафактного программного обеспечения.

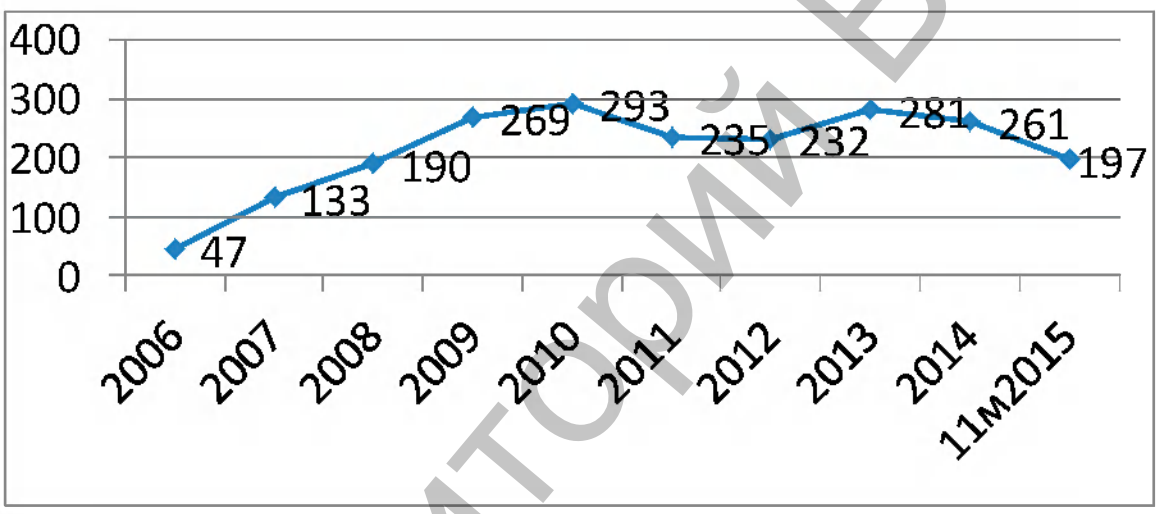
Изучая динамику киберпреступности в Республике Беларусь за последние годы, можно увидеть, что мировая тенденция постоянного

возрастания количества данного вида преступления характерна и для нашей страны.

Количество выявленных преступлений в СВТ
в Республике Беларусь с 2006 по 2015 годы



Количество выявленных преступлений в СВТ
в Витебской области с 2006 по 2015 годы



Культура пользования возможностями электронных помощников у наших граждан пока остается на низком уровне. Отсутствует системное обучение грамотному использованию возможностей сети Интернет, обеспечению собственной безопасности. На фоне доступности компьютерной техники и мобильных устройств, которые, в первую очередь, приобретаются для подрастающего поколения, должный контроль за их использованием со стороны фактических владельцев (родителей) по причине отсутствия необходимых знаний и навыков осуществляется крайне неэффективно, что, в свою очередь, способствует увеличению жертв киберпреступлений и сетевых махинаций.

Развитость национального сегмента сети Интернет находится на низком уровне. Это способствует оттоку веб-пользователей на ресурсы русскоязычного сегмента Сети, расположенные в доменных зонах соседних государств. Последнее чревато увеличением среди белорусских граждан количества жертв киберпреступлений, раскрытие которых нередко связано с трудностями по установлению личности пре-

ступника, его обнаружению и привлечению к ответственности в соответствии с законодательством Республики Беларусь.

Предпосылкой совершения киберпреступлений является ряд психологических аспектов: уверенность злоумышленников в том, что успех дела не связан с большим риском, преступники не могут видеть своих жертв, будь то отдельные люди или целые организации, которые они выбрали для атаки. Такие свойства интернет как трансграничность и анонимность способствуют укоренению подобных убеждений среди начинающих хакеров.

В первую очередь это объясняется тем, что сегодня существует большое количество анонимных интернет-ресурсов, предлагающих от эксплуатации уязвимостей до троянских программ для построения ботнетов (тысячи зараженных компьютеров), а также готовые ботнеты «в аренду». Уровень технической подготовки, необходимый для того чтобы запустить криминальный бизнес, становится все ниже. Появление новых сервисов, доступных через интернет, и миллионы желающих этими сервисами пользоваться также способствуют развитию киберпреступности. Последнее особенно актуально для Республики Беларусь. Как и во всем мире, преступления, совершаемые в виртуальной среде, которые направлены на хищение денежных средств либо сведений, предоставляющих доступ к ним, составляют подавляющее большинство от общего числа выявляемых в нашей стране киберзлодеяний. Их удельный вес уже не первый год колеблется от 80 до 90% от числа всех выявленных IT-преступлений в республике. Так в 2014 году выявлено 2033 подобных хищений. Приведенная ниже пропорция не является особенностью только Республики Беларусь – это мировая тенденция.

Нельзя не отметить тот факт, что значительная часть хищений с банковских пластиковых карт совершаются с использованием подлинных платежных средств, неправомерно вышедших из законного владения потерпевших либо при помощи иных преступных методов. В последние годы наблюдается тенденция к снижению подобного вида преступлений. Связано это, прежде всего, с активной профилактической работой проводимой подразделениями по раскрытию преступлений в сфере высоких технологий МВД во взаимодействии с банками.

К примеру, в 2009 году с целью профилактики хищений денежных средств с картсчетов граждан УВД Витебского облисполкома направило во все банковские структуры предложения по устранению причин и условий, способствующих их совершению, а именно: оснащение всех банкоматов системами видеонаблюдения; внесению изменения в программное обеспечение, требующее подтверждения ПИН-кода после каждой транзакции.

В настоящее время, при активном содействии подразделений по

раскрытию преступлений в сфере высоких технологий МВД, принято Постановление Национального Банка Республики Беларусь о, так называемой, «нулевой ответственности» клиентов банков. Последнее обязывает финансовые учреждения возвращать денежные средства своим клиентам в случаях доказательства их криминального исчезновения с картсчета держателя. В силу принятия данного постановления банки сами стали заинтересованы в профилактике хищений денежных средств клиентов с использованием поддельных банковских карточек, в связи с этим значительная часть банкоматов оборудована антискимерными устройствами, а так же перед снятии денежных средств в банкоматах выводиться предупреждение, что бы клиент убедился в отсутствии посторонних устройств на банкомате.

В целях предупреждения случаев краж денежных средств у владельцев банковских пластиковых карт, обеспечения информационной безопасности интернет-пользователей, а также преодоления правовой неграмотности граждан в данной сфере нашими подразделениями разработаны информационные профилактические аудиоролики, которые направлены в территориальные подразделения для их озвучивания в общественном транспорте, в местах массового скопления граждан областного (районного) центра (вокзал, рынок и т.д.).

Не может не беспокоить и ежегодный прирост преступлений против информационной безопасности (статьи 349-355 УК). К примеру, в 2013–2015 годах в Беларуси отмечен всплеск обращений от граждан, ставших жертвами распространителей вирусов, целью которых является дальнейшее вымогательство денег по следующей схеме. На «зараженном» персональном компьютере потенциальной жертвы блокируется веб-обозреватель, после чего на экране появляется сообщение якобы от имени МВД Республики Беларусь, в котором предлагается уплатить штраф якобы за просмотр и копирование материалов, содержащих элементы педофилии, насилия и гей-порно. Далее приводится информация о том, что в течение суток после уплаты штрафа на указанный в сообщении электронный кошелек, «нарушитель» получит код разблокировки своего браузера. Проведенный анализ денежных сумм, перечисляемых на указанные вредоносной программой электронные кошельки, свидетельствовал о том, что данное явление в республике носит массовый характер. За период активации электронных кошельков (два дня) от пользователей различных регионов республики на номера кошельков были перечислены денежные суммы от двух до четырех миллионов рублей (от 20 до 30 потерпевших с учетом требуемой преступниками разовой выплаты). В связи с этим была осуществлена информационная компания в различных СМИ областного и республиканского уровней, а также на информационных ресурсах сети Интернет.

В материалах была не только разоблачена суть мошеннической

схемы, разъяснен алгоритм действий пользователя в случаях, когда факт перечисления денег уже имел место, но и даны практические рекомендации, направленные на самостоятельную разблокировку операционной системы компьютера.

На наш взгляд, здесь заметную роль сыграл тот факт, что подобные нарушения закона высоко латентны и за помощью в правоохранительные органы обращается не более 20% потерпевших.

В настоящее время нашим подразделением проводиться комплекс оперативно-розыскных мероприятий в отношении жителей Витебской области, причастных к распространению вредоносного программного обеспечения.

Не менее важным аспектом профилактики преступлений в сфере информационных технологий является сама работа правоохранительных органов, связанная с выявлением, раскрытием, расследованием преступлений данной категории. Например из интервью директора ЗАО «Платежная система БЕЛКАРТ» Александра Сотникова – «Международные мошеннические группировки работают с картами международных платежных систем. Кстати, на форумах кардеров (мошенников, которые воруют сведения о банковских картах) достаточно широко распространена информация о том, что в Республике Беларусь поддельные карты лучше не использовать, так как слишком высок процент раскрываемости таких преступлений».

Данному явлению необходимо противопоставить адекватные меры по профилактике и противодействию, составляющими которых являются повышение профессионального уровня сотрудников специализированных подразделений, постоянное совершенствование законодательной базы, создание и подержание единой правоприменительной практики.

Преступлениям в информационной сфере необходимо противопоставить адекватные меры по профилактике и противодействию, составляющими которых являются повышение профессионального уровня сотрудников специализированных подразделений, постоянное совершенствование законодательной базы, создание и подержание единой правоприменительной практики.

На наш взгляд требует совершенствование ряда положений статей главы 31 УК Республики Беларусь, в части оценочного понятия – существенный вред. В настоящий момент нет единого подхода является ли сокрытие или совершение иного преступления существенным вредом.

Не понятна боязнь работников правоохранительных органов при даче юридической оценки совершенным преступлениям. Так при квалификации деяний виновного лица в некоторых районах упорно избегают дачи правовой оценки действиям лица, связанным с изменением, модификацией, блокированием, несанкционированным доступом к компьютерной информации.

Зачастую сотрудникам подразделения приходиться обращаться в прокуратуру Витебской области за помощью в даче надлежащей пра-

вовой оценки, за редким исключением наша позиция по материалам проверок находит поддержку в прокуратуре области.