ствлении оперативно-розыскных мероприятий в направлении борьбы с информационной (в том числе компьютерной) преступностью.

В настоящее время существует программы, которые позволяют:

контролировать процесс попыток взлома компьютерной системы или сети;

определять индивидуальный почерк работы программиста и идентификационные характеристики разработанных им программ;

определять перечень электронных адресов и сайтов интернета, с которыми работал пользователь;

негласно регистрировать перечень программ, с которыми работает пользователь;

определять путь, а в некоторых случаях и конкретный адрес исходящей угрозы для компьютерных систем;

осуществлять негласный контроль над программистом, определяя характер разрабатываемых продуктов;

обнаруживать латентную и закодированную информации в компьютерной системе;

проводить идентификацию компьютерных систем по следам применения на различных материальных носителях информации;

осуществлять исследование следов деятельности оператора в целях его идентификации;

осуществлять диагностику устройств и систем телекоммуникаций на возможность осуществления несанкционированного доступа к ним;

исследовать материальные носители с целью поиска заданной информации;

осуществлять исследование компьютерных технологий для установления возможности решения конкретных преступных задач (крекинг, хакинг, фрикинг и т. п.);

исследовать программы ЭВМ и базы данных с целью определения их возможного предназначения для преступных действий (при наличии программных закладок, подпрограмм класса «троянский конь» и т. п.).

Поисковые программные средства могут найти широкое применение в оперативно-розыскной деятельности (непроцессуальная форма), в том числе и до возбуждения уголовного дела. Факт обнаружения объектов (программы закладок, программное обеспечение для изготовления вирусов или для осуществления взлома компьютерных сетей и т. п.) может послужить основанием для возбуждения дела и производства расследования. В процессуальной форме поисковые программные средства могут найти применение при проведении следственных действий, таких как следственный осмотр (все его виды), выемка предметов, документов и электронной почтовой корреспонденции, следственный эксперимент, выполняемый с целью опытной проверки показаний.

В оперативно-розыскной деятельности при расследовании компьютерных преступлений целесообразно применять криминологическое прогнозирование индивидуального и преступного группового поведения. Определенную информацию можно извлечь, анализируя сетевой трафик локальных и региональных компьютерных сетей. Полезную информацию могут дать и анализ платежей клиентов за телефонные услуги. Прогнозирование может успешно осуществляться в основе первичных материалов оперативного учета, так как его банки информации создаются на основе прогноза вероятности преступного поведения определенных криминогенных контингентов. Все это в совокупности является элементами методики криминологического прогнозирования, которое вплетается в оперативно-розыскные мероприятия при реализации форм оперативно-розыскной деятельности (поиск, профилактика, разработка). Естественно, вопросы моделирования и прогнозирования необходимо решать, используя современные технологии.

Таким образом, мы видим, что почти все виды компьютерных преступлений можно так или иначе предотвратить. Мировой опыт свидетельствует о том, что для решения этой задачи правоохранительные органы должны использовать не только различные профилактические меры, но и активные меры по борьбе с данными преступлениями. Профилактические меры следует воспринимать как деятельность, направленную на выявление и устранение причин, порождающих преступления, и условий, способствующих их совершению, а в целях борьбы следует создавать специальные подразделения, которые будут заниматься раскрытием интернет-преступлений. Для этого сотрудникам правоохранительных органов необходимо получить знания по основам учебных дисциплин в области кибернетики и вычислительной техники.

УДК 006.07

С.В. Пашковский

ОСНОВНЫЕ НАПРАВЛЕНИЯ СОВЕРШЕНСТВОВАНИЯ ЗАКОНОДАТЕЛЬСТВА В ОБЛАСТИ ИНФОРМАЦИОННОЙ БЕЗОПАСНОСТИ

Начав обсуждение вопроса о совершенствовании законодательства в области информационной безопасности, необходимо отметить, что в рамках текущего доклада под информационной безопасностью пони-

мается состояние, достигаемое применением организационных, правовых и технических мер по защите информации, а также систематическим повышением уровня подготовки специалистов, реализующих названные меры. Изменение каждого из этих элементов неизбежно оказывает влияние на остальные. Так, стремительное развитие сферы информационно-коммуникационных технологий требует своевременного редактирования отдельных нормативных правовых актов и технических правовых актов. Учитывая указанное обстоятельство, ОАЦ осуществляет систематическую работу по совершенствованию законодательства в сфере защиты информации.

В ближайшее время развитие названной отрасли законодательства будет определяться тремя основными факторами.

Во-первых, подготовкой и принятием Закона Республики Беларусь «О персональных данных», который позволит однозначно определить понятийный аппарат, категории персональных данных, принципы работы и основы правового регулирования порядка обработки и защиты персональных данных, права субъектов персональных данных и обязанности операторов при их обработке, порядок трансграничной передачи персональных данных, а также установить контроль и ответственность в сфере работы с персональными данными.

Вторым фактором будет выступать принятие новой редакции стандарта Республики Беларусь 34.101.30 «Информационные технологии. Методы и средства безопасности. Объекты информатизации. Классификация». В основе новой классификации объектов информатизации лежат такие признаки, как вид информации в зависимости от категории доступа, наличие подключения к открытым каналам передачи данных, а также конкретный тип информации, распространение и (или) предоставление которой ограничено. Избранный подход формирует множество классов, что позволяет предъявлять более дифференцированные требования по защите информации существующих и перспективных информационных систем.

Третьим фактором является разработка серии стандартов на специализированные средства защиты информации (DLP, SIEM, IPS/IDS), принятие которых позволит существенно снизить стоимость и время прохождения процедуры подтверждения соответствия требованиям технического регламента Республики Беларусь «Информационные технологии. Средства защиты информации. Информационная безопасность» (ТР2013/027/BY), так как исключит необходимость разработки и оценки заданий по безопасности.

УДК 342.951; 351.9; 34:002

Д.В. Перевалов

ПРОБЛЕМНЫЕ ВОПРОСЫ ФУНКЦИОНИРОВАНИЯ СПЕЦИАЛЬНОГО КОМПЛЕКСНОГО АДМИНИСТРАТИВНО-ПРАВОВОГО РЕЖИМА ОБЕСПЕЧЕНИЯ БЕЗОПАСНОСТИ КРИТИЧЕСКИ ВАЖНЫХ ОБЪЕКТОВ ИНФОРМАТИЗАЦИИ

Должное обеспечение безопасности критически важных объектов информатизации (КВОИ) в современных условиях может быть реализовано только в рамках соответствующего специального комплексного административно-правового режима (СКАПР). Формирование такого административно-правового режима обусловлено следующими обстоятельствами.

Во-первых, СКАПР позволяет построить эффективную охрану и защиту соответствующих объектов от различного рода угроз. Во-вторых, он обеспечивает необходимый уровень охраны и защиты соответствующих объектов, что возможно только при наличии должного государственно-управленческого воздействия: общественные отношения, возникающие, изменяющиеся и прекращающиеся в процессе обеспечения безопасности КВОИ, носят преимущественно административно-правовой характер. В-третьих, СКАПР обеспечивает безопасности КВОИ комплексно, так как при его функционировании реализуются нормы сразу нескольких отраслей права – конституционного, международного, административного, уголовного, трудового, а также права технического регулирования; требования и правила данного режима затрагивают различные по характеру права и обязанности субъектов режимного регулирования.

Вместе с тем для СКАПР при обеспечении безопасности КВОИ определяющими являются нормы административного права, поскольку складывающиеся отношения, хоть и относятся к другим правовым отраслям, но в рамках очерчиваемой СКАПР сферы облекаются в административно-правовую форму и становятся объектом административно-правового регулирования.

Однако в виде СКАПР система обеспечения безопасности КВОИ в настоящее время урегулирована нормативно не в должной степени. В то же время в связи с увеличением числа и изменением характера информационных угроз, возрастанием значения КВОИ в жизнедеятельности государства и общества все более актуальной становится потребность в более широком правовом регулировании данной сферы.

Исходя из сложившихся подходов к сущности и содержанию административно-правовых режимов и основываясь на результатах прове-