Информационная безопасность является ключевым фактором сохранения технологического суверенитета государства. Необходимо отметить, что вероятность успешного отражения атаки значительно возрастает, если гражданин способен самостоятельно обнаружить явные признаки атаки на систему безопасности.

В связи с этим фактом представляется актуальной разработка новых и совершенствование существующих программ повышения квалификации сотрудников в области информационной безопасности. Для поддержания и управления уровнем обеспеченности информационной безопасности организации возможно использование концепции киберполигона. В последнее время понятие и термин «киберполигон» привлекли большое внимание. Некоторые исследователи применяют данное понятие для обозначения виртуальной среды, а другие относят киберполигон к физическим составляющим. В общем, полагали, что этим термином возможно обозначить специальную киберлабораторию или среду проведения секретных учений в области информационной безопасности.

Особенностью киберполигона в интересах федерального органа исполнительной власти является его роль в качестве ведомственного высокоэффективного целевого компонента в системе обеспечения информационной безопасности федерального органа исполнительной власти, подведомственных организаций и учреждений.

В связи с этим практически значимым является анализ подходов к реализации научно-технического уровня системотехнических решений, принятых для различных сегментов потребителей, корпоративных применений и органов исполнительной власти с целью формирования совокупности параметров характеристик потребительских свойств киберполигонов.

Сложившаяся практика исследования возможности применения технических решений для киберполигона позволяет получить как предварительные качественные оценки характеристик существенных свойств прототипов объектов техники, так и апробировать походы к оценке их технического уровня.

Особенно важную роль играет апробация для процедур верификации и валидации системотехнических решений по построению киберполигонов, сформированная в ходе исследований совокупность параметров характеристик потребительских свойств киберполигона.

Организационные факторы формирования концептуальных взглядов по построению киберполигона включают в себя:

а) изменения в темпах деятельности и процессов в области информационной безопасности: рост темпов деятельности и скорости бизнес-процессов; минимум времени на реагирование в кризисной ситуации;

б) внедряемые технологии, импортозамещение и достижение технологического суверенитета: цифровизация всех сфер деятельности; изменение ландшафта информационной безопасности; новые технологические риски (киберугрозы);

в) централизацию функций и сервисов в системе обеспечения информационной безопасности: централизация решений; повышение требований к киберустойчивости в связи с агрегацией точек отказа и сокращением цепочки допустимых ошибок;

г) качество результатов: рост целевых показателей; необходимость постоянного повышения эффективности деятельности и дополнительного контроля; усиление негативных последствий от ошибок и сбоев;

д) масштабы деятельности: повышение количества выполняемых операций и увеличение объема информации; расширение территориальной доступности к информационным ресурсам, в том числе облачным сервисам.

Таким образом, киберполигон возможно рассматривать в качестве основы для поэтапного наращивания знаний и компетенций от среднего общего образования до подготовки кадров высшей квалификации, развитие которого обеспечивает актуализацию знаний и компетенций в сфере информационной безопасности граждан на всех уровнях одновременно. Необходимо отметить, что при этом киберполигон позволяет создавать условия, максимально приближенные к реальной жизни, и отрабатывать защиту без риска реального ущерба.

УДК 343.985

А.В. Кезик

ОПЕРАТИВНО-РОЗЫСКНАЯ ПРОФИЛАКТИКА В СФЕРЕ БОРЬБЫ С ПЕДОФИЛИЕЙ

Год от года неизменно усиливает свою актуальность, имеет широкий резонанс в обществе борьба с педофилией. Преступления против половой свободы или половой неприкосновенности несовершеннолетних – наиболее распространенные тяжкие преступления в отношении детей. В области уголовно-правовых отношений важным направлением противодействия таким преступлениям является регламентация защиты половой неприкосновенности или половой свободы несовершеннолетних как особой составляющей обеспечения надлежащего уровня духовно-нравственного и морального развития членов общества. Несмотря на пристальное внимание к указанной категории преступлений со стороны белорусского законодателя, правового сообщества и общественности, многие вопросы правого регулирования таких преступлений в белорусском законодательстве на сегодняшний день остаются неразрешенными и требуют научного анализа, осмысления и обращения к положительному международному опыту правового регулирования.

С развитием информационных технологий, свободного доступа лиц к любой информации, в частности к социальным сетям и свободному неконтролируемому общению в них, а также к информационным ресурсам, на которых имеются видео-, аудиоматериалы о педофилии, деятельность лиц, склонных к совершению преступлений в сфере половой неприкосновенности несовершеннолетних, на территории Минской области, как и в целом в Республике Беларусь, активизировалась. Несмотря на выявленные преступления и количество лиц, привлеченных к ответственности, большая часть преступлений, совершенных в отношении несовершеннолетних в сфере половых отношений, остаются латентными. Следовательно, для их выявления и документирования требуются новые подходы, основанные, в принципе, на уже имеющейся нормативно-правовой базе, регламентирующей оперативно-розыскную деятельность и уголовно-процессуальное производство.

В настоящее время судебно-следственная практика идет по пути привлечения к установленной Законом ответственности только лиц, уже совершивших уголовно-наказуемые деяния, где имеют место быть факты наступления общественно-опасных последствий.

Полагаем, что имеющийся правовой инструментарий в виде Закона Республики Беларусь «Об оперативно-розыскной деятельности» и иных нормативных правовых актов позволяет правоохранительным органам выявлять потенциальных педофилов на ранней стадии совершения ими преступлений и в ходе осуществления оперативно-розыскной деятельности документировать преступные действия последних, не доводя до реальных встреч с несовершеннолетними, тем самым исключая наступление общественно-опасных последствий.

Так, при выявлении и пресечении общественно-опасных деяний по линии борьбы с педофилией, нередко возникает необходимость в проведении комплекса оперативно-розыскных мероприятий, направленных на документирование возможных противоправных действий со стороны определенных совершеннолетних лиц, которые, согласно имеющейся оперативной информации либо заявлению (обращению) граждан, предпринимают попытки личных встреч с несовершеннолетними, заведомо для них не достигшими 16-летнего возраста, или заведомо для них малолетними. Как правило, но не обязательно, подобные фигуранты предварительно общаются с несовершеннолетними (малолетними) посредством сети Интернет (мобильной связи) и часто в процессе своего общения затрагивают сексуальные темы, предлагают обмениваться фотографиями порнографического и эротического характера и т. п., т. е. в их действиях уже усматриваются признаки состава преступления, предусмотренного ст. 169 УК Республики Беларусь («Развратные действия»), относящегося к категории менее тяжких. Вместе с тем, некоторые из данных фигурантов предлагают несовершеннолетним (малолетним) воочию с ними встретиться с мотивировкой «для личного знакомства и более тесного общения», не всегда сразу раскрывая истинных своих намерений. В данном случае, по нашему мнению, задокументировать возможные противоправные действия со стороны указанных фигурантов, т. е. фактически предоставить им возможность проявить свой преступный умысел либо показать отсутствие такового, кроме как посредством проведения соответствующих ОРМ («оперативный опрос», «оперативный эксперимент» и т. п.), не представляется возможным.

Однако, несмотря на все предпринимаемые меры, качественное проведение самого ОРМ, обеспечение безопасности его несовершеннолетних (малолетних) участников, при даче правовой оценки действиям фигуранта следственными подразделениями высказываются большие сомнения по поводу достаточности собранных доказательств при инкриминировании тяжкого либо особо тяжкого состава преступления (даже через покушение), при этом отчетливо осознавая и, соответственно, признавая, что оперативные сотрудники не имели права допустить в действительности наступления общественно-опасных последствий в отношении несовершеннолетних (малолетних) участников ОРМ. В результате чего имеют место факты, когда следственные подразделения, даже возбудив уголовное дело по особо тяжкой статье (ч. 3 ст. 167 УК Республики Беларусь), впоследствии, сомневаясь в данной квалификации, не принимают решение о применении в отношении подозреваемого меры пресечения в виде заключения под стражу, освобождая последнего из МЛС, и в конечном итоге прекращают уголовное дело за отсутствием состава преступления. Сомнения представителей СК основываются на отсутствии подобной правоприменительной практики в республике, когда решение необходимо принимать, рассматривая не уже свершившийся факт преступления, а упрежденный и задокументированный в результате проведенных ОРМ.

Таким образом, в целях решения указанной проблемы необходима дальнейшая координационная работа всех заинтересованных государственных органов по разрешению вопросов оперативно-розыскной профилактики в сфере борьбы с педофилией.

УДК 343.3

О.Н. Ковалёв

ПРОТИВОДЕЙСТВИЕ ДЕСТРУКТИВНОМУ ИНФОРМАЦИОННОМУ ВОЗДЕЙСТВИЮ В СФЕРЕ ЛЕСНОГО ХОЗЯЙСТВА РЕСПУБЛИКИ БЕЛАРУСЬ

За последние два десятилетия в мире появились принципиально новые цифровые средства информации и коммуникации (социальные сети, мессенджеры, медиаплатформы), которые значительно повлияли на все аспекты жизнедеятельности социума. В большинстве стран их трансформация происходит без жесткого государственного контроля, что в условиях современных локальных военных конфликтов, цветных революций, информационных войн создает опасность нанесения ущерба национальным интересам. В таких условиях информационная безопасность государства приобретает все более важное значение.

Проблемам национальной безопасности в информационной сфере посвящены исследования белорусских ученых В.Ю. Арчакова, С.Н. Князева, О.С. Макарова, А.А. Смеяна, Л.С. Мальцева, М.В. Мясниковича, А.Л. Баньковского и др. Современное понимание сущности информационной безопасности закреплено в Концепции национальной безопасности Республики Беларусь, где дано определение понятия «информационная безопасность».

25 марта 2022 г. Президент Республики Беларусь А.Г. Лукашенко на совещании о текущих вопросах деятельности средств массовой информации сообщил следующее: «Идет глобальная информационная война, участниками которой мы являемся... Вы видите, как грубо против нас воюют. Демонизируют официальные Москву и Минск перед остальным миром. Переплюнули уже даже Шарпа и Гебельса. Потоки откровенной, самой наглой, дикой лжи льются на людей из интернета. Забыты все приличия. Про нормы журналистики, профессиональную ответственность уже никто вообще не вспоминает. Это