Так, первая попытка сформулировать определение указанного термина предпринята Н.В. Терзиевым, который считает, что без вести пропавшими считаются лица, безвестно отсутствующие из своего последнего места жительства при криминальных обстоятельствах, покончившие жизнь самоубийством или оказавшиеся жертвой несчастного случая. В.М. Шванков определяет данное понятие как исчезнувшее без видимых к тому причин лицо, местонахождение и судьба которого неизвестны. Указанной позиции придерживается и В.Г. Камыш, который дополняет определение причинами отсутствия информации о местонахождении лица – невозможность либо отсутствие желания сообщить о себе сведения. В.М. Атмажитов, В.А. Лукашов и В.П. Цильник обращают внимание на неожиданность исчезновения лица и наличие заявления в ОВД по факту его исчезновения.

К.К. Горяинов, В.С. Овчинский и Г.К. Синилов к лицам, пропавшим без вести, относят «исчезнувших внезапно без видимых к тому причин, местонахождение и судьба которых для окружающих неизвестны, в том числе: несовершеннолетних, ушедших из дома, школ-интернатов, детских домов, бежавших из центров временной изоляции и специальных образовательных учреждений; психически больных, ушедших из дома или медицинского учреждения, утративших связь с близкими родственниками».

А.И. Гигевич дает авторское определение термину «лицо, пропавшее без вести»: физическое лицо, местонахождение которого неизвестно его родственникам и иным лицам в силу причин медицинского, социального, военного, криминального характера, природных и техногенных катаклизмов, по факту исчезновения которого имеется материал проверки в порядке ст. 172, 173 УПК Республики Беларусь или ВУД в соответствии с п. 2 ст. 167 УПК Республики Беларусь. И.И. Басецкий и В.С. Гайдельцов определяют указанный термин как лицо, о безвестном исчезновении которого поступило заявление или сообщение в ОВД и прокуратуру.

По нашему мнению, наиболее успешными являются позиции А.И. Гигевича, закрепившего в определении рассматриваемого термина элемент правосубъектности, а также И.И. Басецкого и В.С. Гайдельцова, которые не ограничивают приобретение статуса лица, пропавшего без вести, наличием собранных материалов проверки либо уголовного дела, за исключением органов, в которые поступает сообщение или заявление о безвестном исчезновении. Вместе с тем перечисление причин безвестного исчезновения лиц, пропавших без вести, определяет границы данного термина, т. е. нельзя быть уверенным, что указанные причины полностью исчерпывают предметную область. Нецелесообразно также использовать в определении те обстоятельства, которые указывают на отсутствие сведений о местонахождении пропавших лиц, а также на причины отсутствия указанных сведений у родственников либо иных лиц, поскольку для заявителя местонахождение лица может быть неизвестно, а иные лица могут располагать такими сведениями, либо лицо может сообщить о факте безвестного исчезновения с целью сокрытия общественно опасного деяния. Следует также отметить, что задача по розыску лиц, пропавших без вести, возлагается на ОВД, в связи с чем в предлагаемом определении мы будем использовать именно этот орган.

Учитывая вышеуказанные обстоятельства, под лицом, пропавшим без вести, следует понимать физическое лицо, в отношении которого в ОВД поступило заявление (сообщение) об его исчезновении.

Таким образом, имевшая место неопределенность в законодательстве, а именно разделение на статус без вести пропавшего (безвестно исчезнувшего) и исчезнувшего, ранее закрепленное в утратившем силу нормативном правовом акте, была устранена: изменено определение термина «лицо, пропавшее без вести», исключен термин «исчезнувшее лицо».

Данные изменения также способствуют устранению ранее заданных границ рассматриваемого термина; однозначному толкованию указанного термина и выработке единого подхода в действиях сотрудников подразделений уголовного розыска ОВД, что влияет на качество розыска, а также на оптимизацию процесса организации мероприятий по проведению ОРМ на стадии ВУД.

УДК 004.9

А.В. Калач

СОВРЕМЕННЫЕ АСПЕКТЫ ПОДГОТОВКИ ВЫСОКОКВАЛИФИЦИРОВАННЫХ КАДРОВ В СФЕРЕ ИНФОРМАЦИОННОЙ БЕЗОПАСНОСТИ

В результате быстрой цифровизации общества в последние несколько лет наблюдается рост общего количества случаев и появление новых угроз информационной безопасности Российской Федерации, что обусловлено цифровой трансформацией государства и одновременным отставанием развития технологической основы для подготовки специалистов в сфере информационной безопасности, в частности, противодействия кибератакам.

Недавние инциденты в сфере безопасности во всем мире показали, что угрозы кибербезопасности стали сложнее и гораздо серьезнее. Злоумышленники становятся намного организованнее, а векторы атак используют более совершенные и интеллектуальные методы и инструменты. Первой линией защиты от таких атак является повышение осведомленности общественности о кибербезопасности и овладение навыками безопасности среди специалистов по безопасности, чтобы быть готовыми и знать о новейших методах и инструментах угроз. Небезопасное поведение сотрудников остается ключевой проблемой нарушения информационной безопасности в организации, что ведет к значительным финансовым потерям. Установлено, что 57 % атак были совершены сотрудниками, стремящимися продвинуться по карьерной лестнице и покидавшими организацию, количество инсайдерских инцидентов выросло на 47 %, а стоимость этих инсайдерских угроз выросла на 31 %.

В последнее десятилетие тема культуры кибербезопасности граждан вышла на передний план. Осведомленность об обеспеченности информационной безопасности в организации имеет решающее значение для защиты от атак на информационные активы.

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.