во, уголовный процесс, криминалистику, проводить регулярные встречи ученых, представителей правоохранительных органов и частного сектора для обмена опытом и решения проблем, выработки стратегических подходов в борьбе с киберпреступностью, создания учебных и образовательных программ по данной тематике, проведения переподготовки и повышения квалификации следователей, оперативных сотрудников, судей, прокуроров и экспертов, в том числе осуществляющих свою деятельность не только в сфере противодействия преступлениям против информационной безопасности.

Создание и эффективное функционирование Центра позволит повысить качество расследования не только уголовных дел о преступлениях против информационной безопасности, но и иных категорий преступлений, принять дополнительные меры обеспечения защиты собственности и прав граждан, повысить уровень обеспечения информационной и национальной безопасности Республики Беларусь.

Центр должен стать платформой для сотрудничества и координации действий относительно теоретических и практических вопросов борьбы с киберпреступлениями в Беларуси, объединить экспертные знания правоохранителей, ученых, представителей частного сектора, которые смогут внести финансовый вклад в создание и деятельность организации.

В ходе первоначальных мероприятий Центра по совершенствованию действующего законодательства целесообразно с участием заинтересованных ведомств завершить разработку инициированной в 2012 г. Следственным комитетом Стратегии информационной безопасности Республики Беларусь, в которой могут быть определены угрозы в области информационной безопасности и основные мероприятия, направленные на защиту объектов критической инфраструктуры, прав граждан и государства в киберпространстве, предложены пути решения возникающих проблем, совершенствования национального законодательства в области информационной безопасности.

Оценивая опыт создания специализированных подразделений в составе различных международных правоохранительных организаций, в том числе в рамках Интерпола и Европола, занимающихся вопросами расследования киберпреступлений, необходимо рассмотреть вопрос участия белорусских правоохранительных органов, включая сотрудников Центра противодействия киберпреступности, в деятельности таких подразделений, в том числе путем подписания международных соглашений.

УДК 004:34

Т.Г. Чудиловская

ПРОБЛЕМЫ ОБЕСПЕЧЕНИЯ БЕЗОПАСНОСТИ ПРИ ИСПОЛЬЗОВАНИИ ОБЛАЧНЫХ ВЫЧИСЛЕНИЙ В ГОСУДАРСТВЕННОМ УПРАВЛЕНИИ

Развитие аппаратного обеспечения и технологий виртуализации способствуют тому, что технологии облачных вычислений (cloud computing) приобретают все большую популярность.

По определению Национального института стандартов и технологий США (NIST), официально принятому правительством США, облачные вычисления – это модель предоставления возможности удобного, осуществляемого по запросу пользователя сетевого доступа к общему фонду настраиваемых вычислительных ресурсов (таких, как сети, сервера, хранилища данных, программные приложения и услуги), которые могут быть быстро предоставлены и выделены с минимальными управленческими усилиями или взаимодействием с провайдером услуг.

Суть концепции облачных вычислений заключается в удаленном предоставлении конечным пользователям удаленного динамического доступа к услугам, вычислительным ресурсам и приложениям (включая операционные системы и инфраструктуру) через локальную сеть или интернет.

К наиболее востребованным видам облачных вычислений относятся:

SaaS (Software as a service) – программное обеспечение как сервис, т. е. клиенту предоставляется доступ к необходимому программному обеспечению как услуга.

IaaS (Infrastructure as a Service) – инфраструктура ИТ как сервис, т. е. клиенту предоставляется ИТ инфраструктура в соответствии с потребностями пользователей клиента.

PaaS (Platform as a Service) – платформа как сервис, который предназначен для разработки облачных приложений, прежде всего ориентирован на производителей программного обеспечения.

В настоящее время в передовых странах активно обсуждается и продвигается возможность использования потенциала «облачных вычислений» для решения задач в области государственного управления. Облачные вычисления открывают большие возможности использования «облачных сервисов» государственными органами, способствуют внедрению «облачных технологий» на основе стандартов, позволяют консолидировать информационные ресурсы, повышают качество предоставления государственных услуг и одновременно обеспечивают снижение затрат на ИТ.

Для перевода государственных функций в «облако» многими государствами предпринимаются конкретные действия по дальнейшему системному развитию облачных вычислений в соответствии с современным развитием технологий, разрабатываются стратегические планы развития собственных cloud-систем. В Республике Беларусь в соответствии с указом Президента Республики Беларусь от 23 января 2014 г. № 46 «Об использовании государственными органами и иными государственными организациями телекоммуникационных технологий» создается республиканская платформа на основе технологий облачных вычислений, на которой будут размещены программно-технические средства, информационные ресурсы и информационные системы всех государственных органов и иных государственных организаций. Республиканская платформа создается и размещается на базе республиканского центра обработки данных и единой республиканской сети передачи данных (ЕРСПД) и представляет собой программно-технический комплекс для распределенной обработки данных, реализующий технологии облачных вычислений и обеспечивающий взаимодействие с внешней средой. Оператором республиканской платформы является СООО «Белорусские облачные технологии». Порядок использования государственными органами и организациями республиканской платформы, действующей на основе технологий облачных вычислений, утвержден приказом Оперативно-аналитического центра при Президенте Республики Беларусь от 28 марта 2014 г. № 26.

Одним из сдерживающих факторов при работе с облачными ресурсами являются вопросы безопасности – отсутствие контроля над серверами, вычислительными процессами, возможность утечки критично важной информации и пр.

Проблема организации защищенной среды облачных сервисов обусловлена отсутствием принятого большей частью рынка стандарта обеспечения безопасности облачных вычислений. Несмотря на существование разных сертификационных процедур, базирующихся на критериях и требованиях безопасности, единого подхода и методики для обеспечения защищенности облачных вычислений пока нет, нет и единой методики проверки адекватности защиты провайдера подобных сервисов.

Эффективное обеспечение безопасности облачных сервисов возможно при соблюдении баланса между мерами обеспечения информационной безопасности, ответственность за которые несет поставщик услуг, и средствами защиты, применяемыми клиентом. При этом необходимо учитывать требования законов, подзаконных актов и внутриведомственных нормативных документов; определить политику контроля и доступа к хранимым данным в зависимости от их типа; обеспечить конфиденциальность с целью защиты против случайного или злонамеренного доступа к информации; организовать оптимальное управление

данными (поставщики облачных услуг должны предоставлять адекватные средства обеспечения безопасности и контроля).

В набор средств защиты, обеспечивающих безопасность при использовании облачных сервисов, входят:

безопасная регистрация получателя услуги в «облаке»;

аутентификация получателя услуги в «облаке». Для обеспечения более высокой надежности часто прибегают к таким средствам, как токены и сертификаты;

защита обмена информацией между получателем услуги и «облаком». Провайдер, предоставляющий доступ к данным должен шифровать информацию клиента, хранящуюся в центре обработки данных, а также в случае отсутствия необходимости безвозвратно удалять;

электронная подпись данных;

защита от атак, связанных с подменой «облака» («фишинг», «спуфинг» и т. п.);

обеспечение доверенной среды (операционная система, в которой работает получатель услуги, должна быть свободной от вирусов, программ-шпионов и иного вредоносного софта).

УДК 351.74

В.В. Чумак

ЗАКОНОДАТЕЛЬНОЕ ОБЕСПЕЧЕНИЕ ИНФОРМАТИЗАЦИИ МИЛИЦИИ УКРАИНЫ

Последние 20 лет нормативно-правовое обеспечение информатизации милиции Украины вынуждено было развиваться в новых для страны рамках демократии и гласности и, кроме этого, в условиях стремительного производства новейших технологий. Очевидно, в связи с этим некоторые сферы информатизации милиции остаются не до конца урегулированными, что, безусловно, требует проведения анализа содержания нормативно-правовой базы.

Некоторые вопросы относительно указанной проблемы рассматривались в работах А.М. Бандурки, М.В. Ковалева, Ю.Ф. Кравченко, А.Ф. Скакун, А.Г. Фроловой т. п. Однако необходимость дальнейшего научного поиска обосновывается наличием пробелов в нормативном обеспечении, организационных и даже программно-технических недостатков в комплексе мероприятий, направленных на развитие действенной системы информационного обеспечения украинской милиции. Именно данная проблема заставляет определить целью доклада анализ нормативно-правового обеспечения информатизации милиции Украины, ко-