В законодательстве Республики Беларусь имеется ряд нормативных правовых документов, актов, регулирующих отношения, возникающие при использовании информационных ресурсов, включая и интернет-сайты. Так, согласно Указу Президента Республики Беларусь от 1 февраля 2010 г. № 60 «О мерах по совершенствованию использования национального сегмента сети Интернет» на государство возложена обязанность обеспечения защиты интересов личности, общества и государства в информационной сфере, а также создание необходимых условий для дальнейшего развития национального сегмента глобальной компьютерной сети Интернет. Подобный подход закреплен и в Указе Президента Республики Беларусь от 9 ноября 2010 г. № 575 «Об утверждении Концепции национальной безопасности Республики Беларусь», согласно которому информационная безопасность рассматривается как состояние защищенности сбалансированных интересов личности, общества и государства от внешних и внутренних угроз в информационной сфере.

В этой связи Республика Беларусь берет на себя обязательства по обеспечению информационной безопасности, проводит объективный и всесторонний анализ и прогнозирование угроз информационной безопасности нашему государству, разрабатывает меры, направленные на предотвращение, отражение и нейтрализацию информационных угроз.

Исследование современного состояния правоприменительной практики позволяет сделать вывод о наличии тенденции к увеличению числа зарегистрированных преступлений в сфере высоких технологий. Причины роста носят отчасти организационный характер и обусловливаются многообразием форм возможной противоправной деятельности в сети Интернет, а также непрерывным совершенствованием преступниками новых способов и путей для совершения противоправных деяний.

Резюмируя, отметим необходимость совершенствования существующей системы защиты информационной среды, принятия мер превентивного характера в исследуемой сфере. Это может быть обеспечено самыми различными мерами и средствами, начиная от создания климата глубоко осознанного отношения сотрудников к проблеме безопасности и защиты информации до создания глубокой, эшелонированной системы защиты физическими, аппаратными, программными и криптографическими средствами. При этом, разумеется, необходимо соблюдать действующее законодательство, чтобы избежать нарушения личных прав человека и гражданина, гарантированных не только национальными нормативными правовыми актами, но и рядом универсальных международных соглашений.



УДК 343.98.06

***П.В. Лутович, Д.Д. Зык***

## АКТУАЛЬНОСТЬ ИССЛЕДОВАНИЯ КРИПТОГРАФИЧЕСКИХ МЕТОДОВ ЗАЩИТЫ ИНФОРМАЦИИ

Бурное развитие информационных технологий предопределило их использование в преступных целях. Развитие информационных технологий также предопределило использование мер защиты информации от несанкционированного доступа, например, криптографии, используемой различные методы шифрования данных. Для их понимания проведем анализ их развития и внедрения в повседневное пользование.

Симметричное шифрование – это способ шифрования данных, при котором один и тот же ключ используется и для кодирования, и для восстановления информации. До появления асимметричных шифров (1970-е гг.) выступало единственным криптографическим методом. Однако такие простейшие шифры легко взломать – например, зная частотность разных букв в языке, можно соотносить самые часто встречающиеся буквы с самыми многочисленными числами или символами в коде, пока не удастся получить осмысленные слова. С использованием компьютерных технологий такая задача стала занимать настолько мало времени, что использование подобных алгоритмов утратило всякий смысл.

Асимметричное шифрование – это метод шифрования данных, предполагающий использование двух ключей – открытого и закрытого. Открытый (публичный) ключ применяется для шифрования информации и может передаваться по незащищенным каналам. Закрытый (приватный) ключ применяется для расшифровки данных, зашифрованных открытым ключом. Открытый и закрытый ключи представляют собой многорядные числа, связанные между собой определенной функцией.

Электронно-цифровая подпись (ЭЦП) – это последовательность символов, являющаяся реквизитом электронного документа и предназначенная для подтверждения его целостности и подлинности. Электронная подпись содержит в себе сведения о владельце сертификата. В ней также может указываться информация о том, когда и во сколько был подписан документ. Чтобы придать юридическую силу документу и доказать момент создания подписи, пользователь обращается к службе штампов времени. Дата и время появляются на документе при подписании электронной подписью в момент, когда программное

обеспечение ЭЦП обращается к службе штампов времени. При этом сохраняется конфиденциальность, так как служба не видит содержимого документа.

Обладая познаниями в данной сфере, злоумышленники могут предпринимать попытки анонимизации и противодействия правоохранительным органам, а также использовать уязвимости мессенджеров, поддерживающих сквозное шифрование с использованием Signal Protocol и XMPP (например, WhatsApp или Viber) для несанкционированного получения доступа к информации. В то же время использование программного обеспечения, обеспечивающее защиту информации методами полного шифрования, существенно затрудняет процесс сбора данных для их использования в качестве доказательств.

При производстве следственных действий могут быть использованы технические средства и способы обнаружения, фиксации и изъятия следов и вещественных доказательств преступления. На текущий момент внедрение дистанционных методов получения компьютерной информации путем доступа к устройствам памяти, установленным на компьютере, является наиболее перспективным.

Представляется целесообразным использовать возможности, предоставленные Законом Республики Беларусь от 15 июля 2015 г. № 307-З «Об оперативно-розыскной деятельности» для получения и исследования зашифрованной информации, имеющей юридическое значение, а также технологическое совершенствование арсенала специальных средств, применяемых оперативными сотрудниками. С учетом активного развития информационно-коммуникационных технологий, их использования в преступных целях, представляется актуальным при проведении криминалистических исследований рассматривать возможность удаленного получения и анализа зашифрованной информации, а также последующего использования результатов ее исследования в уголовном процессе.

УДК 343.985.8

***В.Ю. Мезяк***

## НЕКОТОРЫЕ АСПЕКТЫ ИСПОЛЬЗОВАНИЯ КРИМИНАЛЬНОГО АНАЛИЗА В БОРЬБЕ С ПРЕСТУПНОСТЬЮ

Приоритетным направлением служебной деятельности оперативных подразделений органов внутренних дел (ОВД) является выявление, предупреждение и пресечение преступлений. Ключевой составляющей в этой деятельности является «криминальный анализ», который представляет собой деятельность по выяснению и пониманию сущности отношений между криминальными и другими данными, потенциально значимыми для ОВД. Целью криминального анализа является поиск оперативно значимой информации в многочисленном потоке данных, а также использование в борьбе с преступностью.

Научные основы криминального анализа были впервые сформулированы в работе Д. Кеннеди-Коллар «Руководство для детективов», подготовленным в целях оказания помощи в совершенствовании навыков у представителей правоохранительных органов. Автором были представлены и обоснованы следующие типы криминального анализа: криминалистическая картография (Crime Mapping); административный и операционный анализ (Administrative and Operational Analysis); стратегический криминальный анализ (Strategic Crime Analysis); разведывательный анализ (Intelligence Analysis); уголовно-следственный анализ (Criminal Investigative Analysis); географическое профилирование (Geographic Profiling); тактический анализ преступлений (Tactical Crime Analysis).

По мнению автора, под криминальной картографией следует понимать создание визуального представления о характеристике места преступления (нанесение на карту, выполненную в цифровом виде, информации о географическом расположении места происшествия в целях анализа влияния на причины противоправных деяний, окружающей обстановки). Сущность административного анализа заключается в визуализации статистических данных о совершенных преступлениях в определенных местах. Стратегический анализ был представлен аналитической обработкой криминалистической информации, содержащейся в базах данных, для установления моделей деятельности правоохранительных органов и их оценки. Уголовно-следственный анализ предусматривает создание профиля неустановленного преступника для его идентификации либо сужения круга лиц, которые могли быть причастны к совершению преступления. Под географическим профилированием понимается оказание помощи правоохранительным органам в идентификации подозреваемых или сужения круга таких лиц, путем анализа сведений о месте совершения преступления.

С учетом приведенной классификации проводимую в настоящее время информационно-аналитическую работу оперативных подразделений ОВД в определенной степени можно соотнести с криминальным анализом. Вместе с тем нужно отметить, что работа в данном направлении зависит от профессиональных интеллектуальных аналитических качеств оперативного сотрудника в выделении необходимой информации из больших массивов данных, направленных на выявление пре-