статей в Уголовном кодексе Республики Беларусь (УК), регламентирующих общественные отношения, касающиеся информационной безопасности, защиты персональных данных, чести и достоинства граждан и вопроса о «фейках» в сети. Приведем их ниже.

Так, в соответствии со ст. 369 «Оскорбление представителя власти» УК предусмотрена уголовная ответственность за оскорбление представителя власти или его близких в связи с выполнением им служебных обязанностей, совершенное в публичном выступлении, либо в печатном или публично демонстрирующемся произведении, либо в средствах массовой информации, либо в информации, размещенной в глобальной компьютерной сети Интернет.

Статьей 391 УК предусмотрено, что оскорбление судьи или народного заседателя в связи с осуществлением ими правосудия наказывается штрафом, или исправительными работами на срок до двух лет, или арестом, или ограничением свободы на срок до трех лет.

В соответствии со ст. 19.11 Кодекса Республики Беларусь об административных правонарушениях предусмотрена административная ответственность за распространение информационной продукции, содержащей призывы к экстремистской деятельности или пропагандирующей такую деятельность, а равно изготовление, хранение либо перевозка с целью распространения такой информационной продукции.

Таким образом, необходимо подчеркнуть, что главным инструментом воздействия на Республику Беларусь является информационно-психологическое воздействие. В этих условиях отсутствие контроля за информационными ресурсами, телеграм-каналами может привести к ложному восприятию информации отдельными гражданами и совершению преступлений. Следовательно, работу по изучению способов ведения информационной войны и совершения киберпреступлений необходимо продолжать. Актуальным остается вопрос о создании военизированных подразделений для противодействия информационным атакам.

УДК 342.732

П.В. Лутович

АКТУАЛЬНЫЕ АСПЕКТЫ РАЗВИТИЯ МЕХАНИЗМОВ ЗАЩИТЫ ГРАЖДАН ПРИ РЕАЛИЗАЦИИ ИМИ ПРАВ И СВОБОД В ИНФОРМАЦИОННОЙ СФЕРЕ

Уровень демократического развития общества определяется не только формальным признанием приоритета прав и свобод человека и

гражданина и их закреплением в национальном законодательстве, но и наличием реальной возможности реализации всего комплекса прав и свобод, гарантированных международными договорами в области прав человека.

Потребности современного общества обусловливают создание эффективно действующего государственно-правового механизма охраны и защиты прав и свобод человека, позволяющий индивиду воспользоваться существующими правовыми и организационными процедурами с целью фактической реализации своих прав и свобод.

Сегодня существующие проблемы защиты прав человека выходят далеко за пределы отдельного государства. Сформировались и получили всеобщее признание международные нормы и принципы в области прав человека, являющиеся стандартом, к достижению которого должны стремиться все государства. Среди основополагающих прав человека ключевую роль в формировании (воспитании) всесторонне развитой личности играет свобода информации, под которой следует понимать группы прав и свобод, включая «свободу выражения убеждений, свободное функционирование средств массовой информации, право общества на получение от государственных служб информации, имеющей общественное значение, свободу распространения информации любым законным способом».

Доступность информации в современных общественных отношениях рассматривается как фактор экономического развития. Особенно это актуально для развивающихся стран, где существуют ограничения по распространению данных в отдельных сферах деятельности. Отсутствие или ограничение предоставления информации создает дополнительные препятствия для функционирования конкурентоспособной экономики, создания эффективного государства и институтов его управления.

Развитие информационных технологий не только облегчают жизнь рядовым гражданам, но и способствуют созданию и производству высокотехнологичных, конкурентоспособных продуктов, пользующихся высоким спросом на международных рынках. Сегодня можно сделать вывод о значительном повышении времени, проводимого различными категориями лиц, в сети Интернет, что объясняется следующим. Современные технологии обеспечивают не только качественное ведение бизнеса, выполнение трудовых обязанностей, но и позволяют эффективно выстраивать коммуникацию.

Вместе с тем в качестве побочного негативного эффекта инновационные процессы способствуют появлению новых угроз противоправного характера, на которые необходимо своевременно реагировать соответствующим правоохранительным органам.

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