Поэтому в схему был внедрен протокол Join. Для этого потребовалось изменить состав ключей членов группы. Они стали содержать три элемента $(A, x, y) \in G_1 \times Z_p^2$, такие, что $A^{x+g} = g_1 h^y$. В свою очередь, это потребовало соответствующей адаптации алгоритмов формирования и проверки подписи. В работе представлено доказательство безопасности адаптированной схемы;

- возможность отзыва сформированных подписей члена группы с заданного момента времени;
- интерактивный процесс формирования подписи с участием удостоверяющего центра.

СПИСОК ЛИТЕРАТУРЫ:

1. *Chaum D., Van Heyst E.* Group signatures // Proceedings of Eurocrypt 1991. Springer-Verlag, 1991. LNCS. Vol. 547. P. 257–265.
2. *Bellare M., Micciancio D., Warinschi B.* Foundations of group signatures: Formal definitions, simplified requirements, and a construction based on general assumptions // Proceedings of Eurocrypt 2003. Springer-Verlag, May 2003. LNCS. Vol. 2656. P. 614–629.
3. *Boneh D., Shacham H.* Group signatures with verifier-local revocation // Proc. 11th ACM Conference on Computer and Communications Security (ACM-CCS'04). 2004. P. 168–177.

И. Р. Бегишев

ОТВЕТСТВЕННОСТЬ ЗА НАРУШЕНИЕ РАБОТЫ ИНФОРМАЦИОННО-ТЕЛЕКОММУНИКАЦИОННЫХ УСТРОЙСТВ, ИХ СИСТЕМ И СЕТЕЙ

Всеобщая информатизация общества все больше влияет на нашу жизнь. В силу этого нарушения работы информационно-телекоммуникационных устройств, их систем и сетей могут привести к катастрофическим последствиям.

Ответственность за нарушение правил эксплуатации ЭВМ установлена законодателем в статье 274 Уголовного кодекса Российской Федерации (далее – УК РФ) «Нарушение правил эксплуатации ЭВМ, системы ЭВМ или их сети». Данная норма является бланкетной и отсылает к нормативноправовым актам, инструкциям и правилам, устанавливающим правила эксплуатации ЭВМ.

При описании объективной стороны данного вида общественно опасного посягательства указание в диспозиции статьи на действие (бездействие) носит общий характер: используются слова «нарушение правил». Конкретное содержание этих правил раскрывается в нормативных актах других отраслей права. Ими могут быть федеральные законы, постановления Правительства Российской Федерации, правила, инструкции, предписания, например такие, как Общероссийские временные санитарные нормы и правила для вычислительных центров, паспорта качества, технические описания и инструкции по эксплуатации, а также инструкции по использованию программ для ЭВМ. Правила эксплуатации ЭВМ могут быть предусмотрены как в общих требованиях по технике безопасности и эксплуатации ЭВМ и периферийных устройств, так и в специальных правилах и инструкциях, регламентирующих особые условия эксплуатации ЭВМ (например, продолжительность работы и последовательность операций) [1].

Нарушение правил эксплуатации ЭВМ может выражаться в двух формах: в несоблюдении установленных правил эксплуатации аппаратного обеспечения ЭВМ, систем ЭВМ или их сети либо в нарушении правил эксплуатации программного обеспечения, предусмотренного для работы ЭВМ, системы ЭВМ или их сети. Так, например, нарушения правил эксплуатации

ЭВМ могут заключаться: в несоблюдении сроков технического обслуживания узлов и агрегатов; в некачественном проведении профилактических работ по обслуживанию ЭВМ и программ ЭВМ; в использовании несертифицированных программных средств; в ошибочных подключениях устройств, оборудования ЭВМ и т. д. [2].

На наш взгляд, для привлечения нарушителей регламента работы информационно-телекоммуникационных устройств, их систем и сетей к уголовной ответственности по статье 274 УК РФ требуется принять общие правила использования информационно-телекоммуникационных устройств, их систем и сетей, которые должны быть обязательными для всех.

По мнению А. В. Сизова, причинение крупного имущественного ущерба не следует рассматривать как тяжкие последствия. Он считает, что если имущественный ущерб нанесен вследствие дезорганизации информационной системы посредством преступных действий, направленных на компьютерную информацию, то данный ущерб будет входить в понятие существенного вреда, предусмотренного частью 1 рассматриваемой статьи. А имущественный вред, причиненный собственнику в результате нарушения правил эксплуатации ЭВМ, системы ЭВМ или их сети, целью которого не являлась информационная безопасность, должен квалифицироваться по совокупности частью 1 статьи 274 УК РФ и по соответствующим статьям главы 21 УК РФ [3].

При определении тяжких последствий в каждом случае должна устанавливаться причинно-следственная связь между нарушением правил эксплуатации ЭВМ, системы ЭВМ или их сети и указанными в диспозиции последствиями. Уничтожение, блокирование или модификация компьютерной информации должны быть следствием нарушения правил эксплуатации ЭВМ, а они, в свою очередь, должны быть причиной наступления тяжких последствий.

Представляется оригинальной позиция А. Ж. Кабановой [4], которая предлагает декриминализировать состав преступления, предусмотренный статьей 274 УК РФ «Нарушение правил эксплуатации ЭВМ, системы ЭВМ или их сети», и перевести указанный состав правонарушения в сферу регулирования административного права.

Думается, что такой перевод в русло административного права невозможен ввиду того, что такие последствия, как уничтожение, блокирование и модификация охраняемой законом цифровой информации, вызванные нарушениями правил эксплуатации информационно-телекоммуникационных устройств, их систем и сетей, в которых такая информация обращается, могут иметь высокую общественную опасность и причинить существенный вред обществу и государству.

Одним из самых распространенных на сегодняшний день способов дистанционной дестабилизации информационно-телекоммуникационных устройств, их систем и сетей является отказ в обслуживании.

Отказ в обслуживании угрожает не самой информации, а автоматизированной системе, в которой эта информация обрабатывается. При возникновении отказа в обслуживании уполномоченные пользователи системы не могут получить своевременный доступ к необходимой информации, хотя имеют на это полное право [5].

Следует отметить, что У. В. Зинина считает диспозицию статьи 274 УК РФ — нарушение правил эксплуатации ЭВМ, системы ЭВМ или их сети — сформулированной как бланкетная, т. е. требующая обращения к конкретным правилам, что затрудняет применение данной статьи в полном объеме в связи с нередким отсутствием соответствующих правил. Более того, общественная опасность этого деяния состоит не в нарушении правил эксплуатации ЭВМ как таковых, что подтверждается анализом зарубежного законодательства, а в тех последствиях, к которым такие нарушения приводят, т. е. в нарушении работы информационных систем или информационно-телекоммуникационных сетей [6].

В то же время ряд исследователей предлагает исключить из УК РФ преступление, предусмотренное статьей 274 УК РФ «Нарушение правил эксплуатации ЭВМ, системы ЭВМ или их сети». К их числу можно отнести Т. Л. Тропина [7] и М. А. Зубова [8].

Аналогичного мнения придерживается и Д. В. Добровольский, который предлагает декриминализировать статью 274 УК РФ путем исключения ее из УК РФ, так как отсутствует реальная необходимость в уголовной наказуемости такого отклоняющегося поведения [9].

Е. В. Красненкова предлагает конкретизировать диспозицию рассматриваемой статьи и изложить ее как «нарушение правил эксплуатации компьютерных и иных автоматизированных электронных систем обработки данных, а также их сетей и систем». Такой подход представляется вполне оправданным, так как он учитывает устоявшуюся сегодня терминологию в сфере безопасности информационных технологий [10].

В связи с вышесказанным, мы предлагаем свое видение рассматриваемой статьи, изложенной в следующей редакции:

«Статья 274. Нарушение работы информационно-телекоммуникационных устройств, их систем и сетей

1. Нарушение работы информационно-телекоммуникационных устройств, их систем и сетей, повлекшее уничтожение, блокирование или модификацию охраняемой законом цифровой информации, — наказывается ...»

СПИСОК ЛИТЕРАТУРЫ:

1. *Дворецкий М. Ю., Копырюлин А. Н.* Правоприменение ст. 274 Уголовного кодекса РФ // Вестник Тамбовского университета. Серия: Гуманитарные науки. 2008. № 2. С. 495.
2. *Кузнецов А. П.* Ответственность за нарушение правил эксплуатации ЭВМ, систем ЭВМ или их сети // Правовые вопросы связи. 2007. № 2. С. 25–29.
3. *Сизов А. В.* Квалификация нарушений правил эксплуатации ЭВМ, системы ЭВМ или их сети // Информационное право. 2007. № 4. С. 27–30.
4. *Кабанова А. Ж.* Преступления в сфере компьютерной информации (уголовно правовые и криминологические аспекты). Автореф. дис. … канд. юрид. наук. Ростов-на-Дону, 2004. С. 6.
5. *Скляров Д. В.* Искусство защиты и взлома информации. СПб.: БХВ-Петербург, 2004. С. 10.
6. *Зинина У. В.* Преступления в сфере компьютерной информации в российском и зарубежном праве. Автореф. дис. … канд. юрид. наук. М., 2007. С. 14.
7. *Тропина Т. Л.* Киберпреступность: понятие, состояние, уголовно-правовые меры борьбы. Автореф. дис. … канд. юрид. наук. Владивосток, 2005. С. 11.
8. *Зубова М. А.* Компьютерная информация как объект уголовно-правовой охраны. Автореф. дис. … канд. юрид. наук. Казань, 2008. С. 14.
9. *Добровольский Д. В.* Актуальные проблемы борьбы с компьютерной преступностью. Автореф. дис. … канд. юрид. наук. М., 2005. С. 9.
10. *Красненкова Е. В.* Обеспечение информационной безопасности в Российской Федерации уголовно-правовыми средствами. Автореф. дис. … канд. юрид. наук. М., 2006. С. 10.

С. В. Белим, Н. Ф. Богаченко

ГРАФ ВЛИЯНИЯ И ЭЛЕМЕНТАРНЫЕ ОПЕРАТОРЫ РОЛЕВОЙ ПОЛИТИКИ БЕЗОПАСНОСТИ

Ролевое разграничение доступа к информации получило широкое распространение не только в системах управления базами данных, но и в операционных системах. Основное отличие ролевой политики безопасности от мандатной и дискреционной состоит в управлении привилегиями. Под привилегией понимается возможность осуществления некоторых действий в системе в целом. Ролевую политику