**УДК 347.77**
**ББК 67.408.135**

**Р.Е. Джансараева,**
*доктор юридических наук, профессор*
*Казахский национальный университет имени аль-Фараби*
**К. Аратулы,**
*магистр юридических наук, докторант PhD*
*Казахский национальный университет имени аль-Фараби*

# БОРЬБА С КИБЕРПРЕСТУПЛЕНИЯМИ: СРАВНИТЕЛЬНЫЙ АНАЛИЗ ЗАКОНОДАТЕЛЬСТВА СТРАН СНГ

В статье анализируется современное состояние законодательного регулирования уголовно-правовых отношений в сфере обеспечения информационной безопасности и практики борьбы с киберпреступлениями. Результативность борьбы с киберпреступлениями обусловлена эффективностью применяемых государством правовых, организационных и кадровых мер. Закономерности в развитии уголовного законодательства об ответственности за преступления в сфере информационных технологий связаны с тенденциями роста киберпреступности. Сравнительный анализ уголовного законодательства ряда государств постсоветского пространства и стран Содружества позволяет сделать вывод о необходимости выработки международной стратегии борьбы с киберпреступностью и унификации национальных законодательств в области уголовно-правового регулирования отношений в сфере информационных технологий и обеспечения информационной безопасности.

*Ключевые слова:* информационная безопасность; борьба с киберпреступностью; киберпреступления; компьютерные преступления; противодействие киберпреступности.

**R.Ye. Dzhansarayeva,**
*Doctor of Law, Professor*
*Al-Farabi Kazakh National University*
**K. Aratuli,**
*Master of Law, Ph.D. student*
*Al-Farabi Kazakh National University*

# FIGHTING CYBERCRIME: COMPARATIVE ANALYSIS OF CIS COUNTRIES' LEGISLATION

The paper analyses the contemporary condition of legislative regulation of criminal law relations in the sphere that ensures information safety and the practice of fighting cybercrime. The results of fighting cybercrime are determined by the effectiveness of legal, organizational and human resources' management actions taken by the state. Regularities in the development of criminal legislation on computer crimes are connected with the cybercrime growth trends. Comparative analysis of criminal legislation in a number of post-Soviet states and CIS countries allows the authors to conclude that it is necessary to work out an international strategy of fighting cybercrime and to unify national legislations which provide criminal law regulation of relations in the sphere of information technologies and provision of information safety.

*Key words*: information security; fighting cybercrime; cybercrimes; computer crimes; counteracting cybercrime.

Современный мир характеризуется динамичными глобальными процессами и трансформацией системы международных отношений. В условиях интеграции и укрепления экономических и политических позиций государств совершенствуются механизмы многостороннего управления, в которых все большую роль играют информационные факторы. Развитие информационной сферы становится одним из ключевых моментов, влияющих на общественное и государственное развитие. От степени развитости информационного общества зависит эффективность функционирования государственных институтов, экономики и обороноспособности государств. Необходимым условием со-

стоятельности государства в условиях современности выступает наличие соотносимого с потребностями граждан информационного общества.

Вместе с тем технологическая эволюция одновременно с позитивом порождает новые проблемы и угрозы информационной безопасности государств, усугубляя существующие. В обстановке глобальной конкуренции информационное давление становится действенным и эффективным методом решения межгосударственных конфликтов. Все интенсивнее используются возможности глобальных информационно–коммуникационных сетей экстремистскими и террористическими организациями для пропаганды и популяризации своей идеологии, распространения радикальных идей, вовлечения все большего числа единомышленников и их обучения, поддержания контактов и финансирования. Информационные системы государств подвержены угрозе компьютерных атак, являющихся одним из способов террористической деятельности. Организованные транснациональные преступные группы все активнее используют современные информационно-коммуникационные технологии в криминальных целях. Меняется динамика киберпреступности – для нее характерна устойчивая тенденция роста.

При этом, несмотря на увеличение зарегистрированных преступлений с использованием современных информационно–коммуникационных технологий, официальная статистика не отражает объективную картину распространения киберпреступлений, показывая лишь незначительную часть реально совершенных. Особенность киберпреступлений заключается в их высокой латентности, появлении новых, изощренных способов совершения преступлений, доказательство которых сильно затруднено из-за отсутствия необходимых правовых, организационных и технических инструментов. Поэтому борьба с киберпреступностью обусловливает потребность соответствующего оперативного реагирования, совместных скоординированных действий спецслужб и правоохранительных органов государств. В этой связи «вопрос о создании новых органов и организаций, координирующих и осуществляющих борьбу с киберпреступностью, что, в свою очередь, требует подготовки национальных кадров, представителей которых можно было бы привлекать на службу в транснациональные органы и организации, направленные на борьбу с киберпреступностью» [1, с. 33], остро стоит на повестке дня не только в России, и Казахстане, но ряде других государств. В Казахстане работу по выявлению, пресечению и раскрытию киберпреступлений, а также преступлений, совершаемых с использованием высоких технологий, осуществляет созданное в 2003 г. в структуре МВД управление «К». Также для системной борьбы с киберпреступлениями в 2006 г. был создан Национальный контактный пункт по борьбе с преступлениями в сфере информационных технологий, который осуществляет постоянный обмен информацией со странами СНГ и дальнего зарубежья.

Квалифицированная кадровая обеспеченность сферы информационной безопасности является одним из основных факторов, влияющих на результативность борьбы с киберпреступностью. Помимо этого необходимо совершенствование процессов и методики обучения, повышения квалификации специалистов, занятых в сфере обеспечения информационной безопасности и борьбы с киберпреступностью.

Для эффективной работы по противодействию киберпреступности требуется правовое обеспечение информационной сферы на государственном уровне, в связи с чем следует обратить особое внимание на правовые механизмы, регулирующие:

– информационные правоотношения, возникающие при поиске, получении, потреблении различной категории информации, информационных ресурсов, информационных продуктов, информационных услуг;

– процессы производства, передачи и распространения информации, информационных ресурсов, информационных продуктов, информационных услуг;

– информационные правоотношения, возникающие при создании и применении информационных систем, их сетей, средств обеспечения, телекоммуникационной инфраструктуры.

Недостаточная согласованность используемых правовых механизмов, фрагментарность деятельности субъектов законодательной инициативы по их развитию и совершенствованию, недостаточная эффективность, противоречивость правовых норм,

характерная для нынешнего состояния правового обеспечения противодействия киберпреступлениям, в совокупности создают серьезную угрозу информационной безопасности государства, которая в структуре Уголовного кодекса Республики Казахстан (далее – УК РК) не получила статуса обособленного объекта уголовно-правовой охраны. В УК РК статья 227 «Неправомерный доступ к компьютерной информации, создание, использование распространение вредоносных программ для ЭВМ» (с изменениями, внесенными Законом РК от 21 декабря 2002 г. № 363) помещена в главу 7 «Преступления в сфере экономической деятельности», «затерявшись» среди деяний, объектом посягательства при совершении которых являются отношения в сфере экономической деятельности. Ответственность по части 1 статьи 227 УК РК предусмотрена за «неправомерный доступ к охраняемой законом компьютерной информации, т. е. информации на машинном носителе, в электронно-вычислительной машине (ЭВМ), системе ЭВМ или их сети, а равно нарушение правил эксплуатации ЭВМ, системы ЭВМ или их сети лицами, имеющими доступ к ЭВМ, к системе ЭВМ или их сети, если это деяние повлекло уничтожение, блокирование, модификацию либо копирование информации, нарушение работы ЭВМ, системы ЭВМ или их сети».

Повышенная ответственность наступает по части 2 статьи 227 УК РК в случае совершения деяния группой лиц по предварительному сговору или организованной группой либо лицом с использованием своего служебного положения.

В части 3 статьи 227 УК РК уголовная ответственность установлена за «создание программ для ЭВМ или внесение изменений в существующие программы, заведомо приводящих к несанкционированному уничтожению, блокированию, модификации либо копированию информации, нарушению работы ЭВМ, системы ЭВМ или их сети, а равно использование либо распространение таких программ или машинных носителей с такими программами». Если эти действия повлекут по неосторожности тяжкие последствия, то ответственность наступает по части 4 статьи 227 УК РК.

В соответствии с Законом РК от 8 января 2007 г. № 210 (с изменениями, внесенными законами РК от 10 декабря 2009 г. № 227–IV; от 18 января 2011 г. № 393–IV) Уголовный кодекс дополнен статьей 227–1 «Неправомерное изменение идентификационного кода абонентского устройства сотовой связи, устройства идентификации абонента, а также создание, использование, распространение программ для изменения идентификационного кода абонентского устройства».

Ответственность в указанной норме предусмотрена за «неправомерное без согласия производителя или законного владельца изменение идентификационного кода абонентского устройства сотовой связи, создание дубликата карты идентификации абонента сотовой связи» (часть 1 статьи 227-1 УК РК), а также за «неправомерные создание, использование, распространение программ, позволяющих изменять идентификационный код абонентского устройства сотовой связи или создавать дубликат карты идентификации абонента сотовой связи» (часть 2 статьи 227-1 УК РК). Совершение указанных деяний группой лиц по предварительному сговору либо организованной группой, либо неоднократно предусматривает ответственность по части 3 статьи 227-1 УК РК. Ввиду указанного расположения норм, предусматривающих ответственность за киберпреступления, т. е. в главе «Преступления в сфере экономической деятельности», отдельного их учета в РК не ведется. Аналогичный подход наблюдается и в уголовном законодательстве Узбекистана: состав преступления «Нарушение правил информатизации» (статья 174) отнесен к преступлениям против собственности и предусмотрен в главе «Хищение чужого имущества» УК Узбекистана.

По-разному определяется родовой объект киберпреступлений в уголовном законодательстве стран СНГ и некоторых государств постсоветского пространства. В Уголовных кодексах России (глава 28, статьи 272–274), Азербайджана (глава 30, статьи 271–273), Кыргызстана (глава 28, статьи 289–291), Туркменистана (глава 33, статьи 333–335), Армении (раздел 9, глава 24, статьи 251–257) и Эстонии («Преступления в сфере компьютерной информации», статьи 268–274) в отдельных главах объединены нормы об уголовной ответственности за преступления в сфере компьютерной информации (безопасности компьютерной информации – УК Армении). Уголовное законодательство Республики Беларусь (раздел XII, глава 31,

статьи 349–355) и Таджикистана (раздел XII, статьи 298–304) предусматривает в качестве родового объекта киберпреступлений информационную безопасность, объединив общественно опасные деяния в главу (раздел) «Преступления против информационной безопасности». Возникают трудности в определении родового объекта киберпреступлений, подлежащих уголовно–правовой охране по УК Грузии (глава 35 «Компьютерные преступления», статьи 284–286) и Молдовы (глава «Преступления в сфере информатики», статьи 259–261). В УК Украины родовой объект определен как отношения в сфере использования ЭВМ (компьютеров), систем и компьютерных сетей, и общественно опасные деяния объединены в разделе XVI «Преступления в сфере использования ЭВМ (компьютеров), систем и компьютерных сетей» (статьи 361–363, 361-1, 361–2, 361–3).

Анализ показывает, что национальное уголовное законодательство государств в сфере ответственности за киберпреступления характеризуется относительным разнообразием. Развитие и изменение национального законодательства по борьбе с киберпреступностью в вышеназванных государствах обусловлены появлением и тенденциями развития киберпреступности, и при подробном анализе обнаруживаются лишь некоторые закономерности. Совершенствование информационных технологий и проникновение их во все сферы человеческой жизнедеятельности ведет к возникновению новых форм преступных посягательств и криминализации новых деяний, а это, в свою очередь, к необходимости выработки эффективных мер борьбы с ними, внесению изменений в уже существующее уголовное законодательство и принятию новых норм.

Бесспорно, эффективное международное сотрудничество в борьбе с киберпреступностью невозможно, если в законодательстве одной страны деяние считается преступлением, а в другой – уголовной ответственности не предусмотрено. Отсутствие единообразия в национальном уголовном законодательстве стран может негативно отразиться на развитии методов эффективной борьбы с киберпреступностью – явлением, для которого не существует государственных границ. Наличие глобальных информационных сетей стирает границы информационного пространства, а «виртуальные» границы между государствами легко пересекаются киберпреступниками, орудующими в любом месте киберпространства, независимо от юрисдикции государств, с помощью компьютера и доступа в Интернет. Эффективное противостояние киберпреступности, учитывая ее трансграничный характер, невозможно, если расследование преступлений, выдача правонарушителей, их преследование в суде затруднены или вообще неосуществимы из–за «нестыковок» в национальном уголовном законодательстве отдельных стран. Фактически, эти различия ограждают киберпреступников от преследования, являясь своеобразным «барьером», позволяют уйти от ответственности, оставляя безнаказанными их деяния.

Вследствие этого государства, прилагающие усилия для защиты своих граждан от киберпреступников, тратят их впустую. С другой стороны, из-за различий уголовно–правового регулирования отношений в сфере информационных технологий лица, соблюдающие законы своего государства, могут подвергнуться уголовному преследованию в другом. Такая ситуация диктует потребность выработки международной стратегии борьбы с киберпреступлениями и унификации национальных законодательств в области уголовно–правового регулирования отношений в сфере информационных технологий.

Приходится констатировать, что законодательное регулирование анализируемых отношений в уголовно-правовой сфере отстает от стремительного развития компьютерных технологий. В настоящее время ответственность за киберпреступления в уголовном законодательстве не отражает глобальных перемен в непрерывном, стремительном процессе информационного развития человечества. Уголовное законодательство недостаточно эффективно регулирует отношения, складывающиеся при совершении киберпреступлений, вследствие чего не реализуются его охранительные и предупредительные функции. Уголовная ответственность в законодательстве Казахстана, как и в законодательстве некоторых государств СНГ, предусмотрена за компьютерные преступления, т. е. за преступления, которые совершаются в отношении компьютеров и компьютерной информации, при этом деяния, которые совершаются с их использованием и посягают на другие объек-

ты уголовно–правовой охраны, остаются вне сферы уголовной ответственности. В уголовном законодательстве Казахстана сегодня сложилась ситуация, когда отношения в сфере информационной безопасности требуют криминализации ряда общественно опасных деяний и самостоятельной охраны названных отношений в отдельной главе Особенной части Уголовного кодекса. Наиболее удачным ориентиром в этом вопросе нам представляется раздел XII «Преступления против информационной безопасности» Модельного кодекса государств–участников СНГ, который содержит семь статей:

– «Несанкционированный доступ к компьютерной информации»

– «Модификация компьютерной информации»

– «Компьютерный саботаж»

– «Неправомерное завладение компьютерной информацией»

– «Изготовление и сбыт специальных средств для получения неправомерного доступа к компьютерной системе или сети»

– «Разработка, использование и распространение вредоносных программ»

– «Нарушение правил эксплуатации компьютерной системы или сети».

## СПИСОК ИСПОЛЬЗОВАННОЙ ЛИТЕРАТУРЫ

1. *Протасевич А.А., Зверянская П.П.* Борьба с киберпреступностью как актуальная задача современной науки // Криминологический журнал Байкальского государственного университета экономики и права. – 2011. – №3. – С. 28–33.

## REFERENCES

1. Protasevich A.A., Zveryanskaya P.P. *Kriminologicheskij zhurnal Bajkal'skogo gosudarstvennogo universiteta ekonomiki i prava* [Criminology Journal of Baikal National University of Economics and Law]. 2011, no. 3, pp. 28-33.

### Информация об авторах

**Джансараева Рима Еренатовна** (Алматы) – доктор юридических наук, профессор, заведующая кафедрой уголовного права, уголовного процесса и криминалистики. Казахский национальный университет имени аль-Фараби (050040 Республика Казахстан, г. Алматы, пр-т аль-Фараби, 71, e-mail: jansarayeva@mail.ru)

**Аратулы Куаныш** (Алматы) – магистр юридических наук, докторант PhD кафедры уголовного права, уголовного процесса и криминалистики. Казахский национальный университет имени аль-Фараби (050040 Республика Казахстан, г. Алматы, пр-т аль-Фараби, 71, e-mail: kunya8585@mail.ru)

### Information about the authors

**Dzhansarayeva, Rima Yerenatovna** (Almaty) – Doctor of Law, Professor, Head, Chair of Criminal Law, Criminal Process and Criminalistics. Al-Farabi Kazakh National University (Al-Farabi pr., 71, Almaty, 050040, Republic of Kazakhstan, e-mail: jansarayeva@mail.ru)

**Aratuli, Kuanish** (Almaty) – Master of Law, Ph.D. student, Chair of Criminal Law, Criminal Process and Criminalistics. Al-Farabi Kazakh National University (Al-Farabi pr., 71, Almaty, 050040, Republic of Kazakhstan, e-mail: kunya8585@mail.ru)