

*Смирнова И. Г., заведующая кафедрой криминалистики и судебных экспертиз Байкальского государственного университета экономики и права (г. Иркутск), доктор юридических наук*

### **ЗНАЧЕНИЕ ПРЕЗУМПЦИИ НЕВИНОВНОСТИ В БОРЬБЕ С КИБЕРПРЕСТУПЛЕНИЯМИ<sup>1</sup>**

В соответствии с утвержденной Указом Президента РФ «Стратегией национальной безопасности Российской Федерации до 2020 г.» национальной безопасностью является состояние защищенности личности, общества и государства от внутренних и внешних угроз, которое позволяет обеспечить конституционные права, свободы, достойные качество и уровень жизни граждан, суверенитет, территориальную целостность и устойчивое развитие Российской Федерации, оборону и безопасность государства.

Под угрозой национальной безопасности следует понимать прямую или косвенную возможность нанесения ущерба конституционным правам, свободам, достойному качеству и уровню жизни граждан, суверенитету и территориальной целостности, устойчивому развитию государства, его обороне и безопасности.

Развитие компьютерных технологий вызвало появление и активное распространение таких общественно опасных преступлений, как киберпреступления.

Так, по данным Главного информационного центра МВД России, в 2004 г. было совершено 13 723 компьютерных правонарушений, что почти в два раза больше по сравнению с 2003 г. (7 053), и их количество неуклонно растет. По словам руководителя Бюро специальных технических мероприятий МВД России А. Мошкова, в сфере высоких технологий именно мошенничества являются самыми распространенными преступлениями в IT-среде, и их количество растет с каждым годом. Если в 2010 г. было возбуждено 736 таких уголовных дел, то за 9 месяцев 2011 г. их число превысило 1 тысячу, при том, что уровень латентности этих преступлений весьма высок. Не менее тревожные тенденции характеризуют состояние преступности и в других государствах.

Бесспорно, что совершение киберпреступлений самым непосредственным образом влияет на состояние защищенности жизненно важных интересов субъектов охраны. Более того, из определения национальной безопасности видно, что круг жизненно важных интересов включает в себя интересы трех основных уровней:

- 1) частные;
- 2) общественные;
- 3) государственные.

В этой связи следует признать, что киберпреступления влияют на степень защиты всех трех групп интересов. Так, в соответствии со ст. 2 Конституции РФ права и свободы человека и гражданина являются высшей ценностью в государстве. К таковым относятся неприкосновенность личности, неприкосновенность жилища и, наконец, тайна (неприкосновенность) частной жизни. Очевидно, что имущественное положение лица связано с его частной жизнью и является составляющей банковской тайны, которая подлежит самостоятельной государственной защите. В свою очередь, уровень общественной напряженности детерминирует нестабильность в государстве, а киберугрозы могут быть направлены на получение сведений, составляющих государственную тайну. И если во многих сферах государственной деятельности конфликт частных и публичных интересов неизбежен, то в случае совершения киберпреступлений в одинаковой степени страдают и частные, и государственные, и общественные интересы.

---

<sup>1</sup> Статья выполнена в рамках реализации договора № 14.Z56.14.2691-МД об условиях использования гранта Президента Российской Федерации для государственной поддержки молодых российских ученых с организациями-участниками конкурсов, имеющими трудовые отношения с молодыми учеными МД-2691.2014.6

Рост киберпреступлений во всем мире, необходимость консолидации усилий государств в борьбе с ними требуют унифицировать национальное законодательство и учитывать позитивный опыт иностранных государств в этой сфере.

Большинству уголовно-процессуальных законов государств известен принцип презумпции невиновности. Согласно ст. 49 Конституции РФ, ст. 14 УПК РФ обвиняемый считается невиновным, пока его виновность в совершении преступления не будет доказана в установленном законом порядке и подтверждена вступившим в законную силу приговором суда. Следовательно, данная презумпция по своей природе является юридической, опровержимой, универсальной. Вместе с тем, если обратиться к законодательству иностранных государств, то можно заметить, что, в соответствии с основными началами доказательственного права в уголовном процессе, например, Франции с презумпцией невиновности непосредственно связаны правила распределения бремени доказывания. Действительно, пока лицо не признано виновным доказать его вину должна сторона обвинения. Вместе с тем, такая обязанность не является абсолютной, поскольку наличие некоторых обстоятельств должна доказывать сторона защиты. Так, например, именно защита обязана доказывать наличие обстоятельств, исключающих преступность деяния, наличие иммунитета от уголовной ответственности и т. п.<sup>1</sup>

Кроме того, возложение бремени доказывания на защиту возможно по определенным категориям уголовных дел. Думается, что с учетом степени общественной опасности по делам о киберпреступлениях возможно также переложение бремени доказывания виновности лица на сторону защиты. Аргументация в пользу расширения подобным образом уголовно-процессуальных механизмов борьбы с киберпреступностью может быть следующей.

Во-первых, ст. 15 УПК РФ закрепляет состязательность сторон как принцип уголовного судопроизводства, что означает необходимость распространения его действия не только на судебное, но и досудебное производство. Однако в настоящее время, несмотря на указание в законе (ч. 3 ст. 86 УПК РФ) на право защитника собирать доказательства, параллельное адвокатское расследование не получило своего развития в уголовном судопроизводстве России.

Во-вторых, действие правил допустимости доказательств следует рассматривать как возможную процессуальную санкцию, применяемую к стороне обвинения за нарушение уголовно-процессуального закона при собирании доказательств. Давая стороне защиты больше полномочий по собиранию доказательств, мы снимаем нагрузку с правоприменителя по разрешению процессуальных конфликтов, связанных с оценкой допустимости доказательств и разрешением вопроса о возможности их последующего использования в процессе доказывания.

В-третьих, последние изменения и дополнения УПК РФ с завидным постоянством демонстрируют тенденцию к упрощению этапа собирания доказательств (дознание в сокращенной форме, особый порядок судебного разбирательства при согласии обвиняемого с предъявленным ему обвинением, особый порядок судебного разбирательства при заключении досудебного соглашения о сотрудничестве и т. п.). Данные особые производства сопряжены с возможностью не проводить все следственные, процессуальные действия. Предлагаемое распределение бремени доказывания логично вписывается в общую концепцию современного уголовно-процессуального законодательства и практики его применения по упрощению этапа собирания доказательств.

Думается, что внедрение указанных предложений будет способствовать борьбе с киберпреступлениями, а также выполнять серьезную профилактическую функцию.

---

<sup>1</sup> Гуценко К. Ф. Уголовный процесс западных государств. — М., 2002. — С. 315–316.