Н.А. Нугманов
Кандидат юридических наук

ЗАКОНОДАТЕЛЬСТВО ЕВРОПЕЙСКИХ ГОСУДАРСТВ ОБ ОБЕСПЕЧЕНИИ ИНФОРМАЦИОННОЙ БЕЗОПАСНОСТИ В КИБЕРПРОСТРАНСТВЕ

Современные процессы глобализации наряду с положительными аспектами несут в себе и отрицательные моменты. Глобализация послужила объединению разрозненных информационных сетей и появлению всемирной виртуальной информационной сети Интернет, ставшего одним из наиболее значительных достижений человечества. С его помощью люди, организации и государства могут в реальном времени обмениваться информацией, данными, включая аудио- и видеозаписи. Таким образом, Интернет явился значительным прорывом в информационной сфере.

Вместе с тем появление информационного киберпространства несет в себе и весьма существенные угрозы. Широкое использование в повседневной жизни компьютерных технологий и создание на их основе глобальных компьютерных сетей как неотъемлемой части современной международной финансовой и банковской деятельности создают предпосылки, облегчающие совершение преступных деяний, которые зачастую остаются безнаказанными. Распространение компьютерных вирусов и детской порнографии, мошенничества с пластиковыми платежными карточками, хищение денежных средств с банковских счетов, компьютерный терроризм – это далеко не полный перечень подобных преступлений, которые получили распространенное название "киберпреступность". При этом наблюдается опасная тенденция сращивания киберпреступности с организованной транснациональной преступностью[1].

По нашему мнению, незаконные действия в киберпространстве могут быть разделены на две большие группы:

1) киберпреступность;

2) кибертерроризм.

Хотя некоторые ученые и относят кибертерроризм к киберпреступности, однако мы считаем, что данный вид должен рассматриваться отдельно от других разновидностей киберпреступности (незаконные операции с кредитными карточками, распространение опасных компьютерных вирусов, троянов, порнографии и мн. др.), ибо по своим последствиям и масштабам наносимого ущерба кибертерроризм стоит особняком.

Одной из новых и опасных угроз человечеству в XXIв. становится использование террористическими организациями информационных технологий и глобальной сети Интернет. Как отмечает Д.Ф.Рахимов, "кибертерроризм представляет собой преднамеренную политически мотивированную атаку на информацию, вычислительные системы, компьютерные программы или данные, совершаемую субнациональными группировками или тайными агентами, результатом которой является насилие против мирных мишеней, создающую опасность гибели людей, причинения значительного имущественного ущерба либо наступления иных общественно опасных последствий"[2].

В.А. Голубев понимает под кибертерроризмом "преднамеренную атаку на информацию, обрабатываемую компьютером, компьютерную систему или сети, которая создает опасность для жизни и здоровья людей или наступление других тяжких последствий, если такие действия были совершены с целью нарушения общественной безопасности, запугивания населения или провокации военного конфликта"[3].

Эксперт в области исследования компьютерной преступности Д. Деннинг в своей книге "Активность, хактивизм и кибертерроризм: Интернет как средство воздействия на внешнюю политику" пишет: "Является ли кибертерроризм терроризмом будущего? Для террористов электронные средства представляют некоторое преимущество по сравнению с физическими. С их помощью можно действовать отдаленно и анонимно, они дешевы, не требуют взрывчатых веществ и миссий самоубийц. Такие теракты, вероятно, получили бы широкую огласку в СМИ, поскольку и журналисты, и публика заинтересуются виртуальным нападением"[4].

Итак, кибертерроризм представляет собой целый ряд важных вызовов:

во-первых, в силу их внутреннего характера компьютерные атаки практически невозможно прогнозировать или проследить в реальном времени;

во-вторых, из-за сложности законов, действующих во всем мире, сбор доказательств в таких обстоятельствах, когда могли быть использованы Интернет или другие электронные средства, а также преследование по закону, поиск, захват и выдача отдельных лиц представляются проблематичными.

Указанные проблемы актуализируют необходимость осмысления существующих и выработки новых механизмов борьбы с кибертерроризмом.

Предупреждение терроризма является чрезвычайно сложной задачей, поскольку это явление порождается многими социальными, политическими, экономическими, историческими, психологическими и иными причинами. От того, насколько точно будут установлены причины этого особо опасного преступления, зависит эффективность мер по борьбе с ним и их дальнейшее совершенствование.

Компьютерная преступность и кибертерроризм представляют собой особую общественную национальную и международную опасность, ибо они являются особым измерением террористической деятельности со специфической причинной базой, для контроля над которой и борьбы с ней необходимы особые меры.

Следовательно, необходимо закрепить на законодательном уровне как меры по обеспечению безопасности компьютерных сетей, так и меры ответственности за нападения на них.

В этой связи представляется актуальным рассмотрение законодательного опыта пресечения актов кибертерроризма европейскими государствами, которые в течение последних лет на законодательном уровне

---

[1] Голубев В. Вопросы международного сотрудничества в борьбе с транснациональной компьютерной преступностью // Преступность и право. М., 2004. № 4. С.36.

[2] Рахимов Д.Ф. Современные конструкции определения терроризма: международно-правовые аспекты // Qonun Himoyasida. Ташкент, 2004. С.82.

[3] Голубев В.А. Кибертерроризм – угроза национальной безопасности. http://www.crime-research.ru/articles/Golubev_Cyber_Terrorism

[4] Dorothy E. Denning. Activism, Hacktivism, and Cyberterrorism: The Internet as a Tool for Influencing Foreign Policy. New York: Marshall Publishers, 2004. P.42.

закрепили ряд прогрессивных положений по пресечению актов кибертерроризма.

Франция. Уголовный кодекс Франции, вступивший в силу 1 марта 1993 г., содержит две статьи, касающиеся киберпреступлений: ст.ст. 186 и 323[1].

Статья 186-1 содержит положения об уголовной ответственности за неправомочный перехват данных в телекоммуникационных системах. За совершение этого преступления установлена ответственность в виде штрафа или лишения свободы на срок до 1 года. Если субъектом преступления является должностное лицо, то срок лишения свободы может быть увеличен до 5 лет.

Часть 1 ст. 323 предусматривает уголовную ответственность за неправомерный доступ к автоматизированной системе обработки данных или части этой системы, если в результате доступа были уничтожены или изменены данные, содержащиеся в системе или нарушено/изменено функционирование системы. Ответственность по данной статье может наступить за создание вредоносных программ, попытку вторжения в системы, незаконный доступ к данным, незаконный доступ к системам связи. За совершение этих преступлений предусмотрена ответственность в виде штрафа или лишения свободы на срок до 2 лет.

Часть 2 ст. 323 определяет в качестве преступления изменение данных или любое вмешательство в автоматизированные системы обработки данных. Часть 3 этой же статьи посвящена изменению данных в системах с целью подлога или мошенничества. За указанные преступления определено наказание в виде штрафа или лишения свободы сроком до 3 лет.

Германия. Уголовный кодекс Германии имеет множество различных статей, в соответствии с которыми можно привлечь к ответственности за компьютерные преступления, но основные из них две – ст. ст. 202 и 303[2].

Пункт "a" ст. 202 предусматривает уголовную ответственность за незаконное получение лицом данных, которые предназначались не для него и находятся под специальной защитой от неправомочного доступа, с целью извлечения выгоды для себя или для третьего лица. При этом указывается, что эта статья распространяется только на данные, содержащиеся на электронных и магнитных носителях или иных носителях, *не видимые непосредственно*. Т.е. эта статья касается только таких данных, как компьютерные данные. Наказание за данное преступление предусмотрено в виде штрафа или лишения свободы сроком до 3 лет.

Пункт "a" ст. 303 касается изменения данных. Он предусматривает, что наказанию в виде штрафа или заключения сроком до 2 лет подлежат стирание, уничтожение, приведение в негодность, изменение данных или попытки произвести такие действия. Эта статья также распространяется только на данные, указанные в ст. 202.

Пункт "b" ст. 303 охватывает такие преступления, как DNS-атаки (компьютерный саботаж) и создание вредоносных программ. Указано, что компьютерный саботаж – вмешательство в обработку данных, существенную для предприятия, государственных органов или чьего-либо способа ведения бизнеса, – является преступлением. Такое вмешательство может быть осуществлено способами, отмеченными в п. "a" ст. 303, либо путем уничтожения, повреждения, приведения в негодность, изменения компьютерной системы, либо вмешательства в передачу данных. Указанные деяния наказываются штрафом или лишением свободы на срок до 5 лет. Покушение на это преступление также наказуемо.

Италия. Уголовный кодекс Италии включает в себя достаточное количество статей, предусматривающих ответственность за киберпреступления[3].

В частности, ч. 3 ст. 615 УК Италии запрещает неправомочный доступ к компьютеру или телекоммуникационной системе, т.е. доступ к компьютерам или системам, защищенным мерами безопасности, либо доступ против выраженного или подразумеваемого желания владельца исключить подобный доступ. Санкция за эти деяния предусмотрена в виде лишения свободы на срок до 3 лет.

Наказание в виде лишения свободы на срок от 1 до 5 лет установлено за совершение такого преступления должностным лицом или лицом, злоупотребившим своими полномочиями, лицом, занимающимся, даже без лицензии, частной детективной деятельностью, а также оператором системы. То же наказание предусмотрено и в случае, если преступление совершено с применением насилия, угрозой причинения вреда имуществу, с применением оружия, если преступление причинило вред системе, частично или полностью прервало ее работу, разрушило или повредило данные, информацию или программы, содержащиеся в системе.

И, наконец, особо квалифицирующими признаками этого преступления являются совершение его в отношении компьютеров или телекоммуникационных систем оборонного значения, а также предназначенных для охраны общественного порядка и общественной безопасности, охраны иных интересов общества. В этом случае наказание составляет от 3 до 8 лет лишения свободы.

Часть 4 ст. 615 посвящена незаконному владению и распространению кодов доступа к компьютерам и телекоммуникационным системам. Согласно этой норме, лицо, с целью получения прибыли для себя или для третьих лиц, либо с целью причинения ущерба производящее, передающее, сбывающее коды, пароли или иные средства доступа к компьютеру или телекоммуникационным системам, а также предоставляющее информацию или инструкции для упомянутых целей, подлежит наказанию в виде штрафа или лишения свободы сроком до одного года.

Часть 5 ст. 615 УК Италии предусматривает ответственность – штраф или лишение свободы на срок до двух лет – за распространение программ, предназначенных для повреждения или уничтожения компьютерных систем. Она устанавливает, что уголовной ответственности подлежат незаконная передача или сбыт компьютерной программы, целью или эффектом которой является повреждение компьютера или телекоммуникационной системы, содержащихся в них программ или данных, а также частичным или полным изменениям или остановкам работы компьютера или телекоммуникационной системы.

Часть 2 ст. 420 УК Италии определяет в качестве

[1] См. подробнее: Уголовный кодекс Франции // Зарубежное законодательство в борьбе с терроризмом / Отв. ред. И.С. Власов. М., 2005.

[2] Уголовный кодекс ФРГ / Пер. с нем. М., 2000. С.112, 176.

[3] См. подробнее: Уголовный кодекс Италии / Пер. с итал. М., 2002.

преступления повреждение или уничтожение общественных информационных инфраструктур, общественных баз данных или программ, задействованных на предприятиях коммунального обслуживания. За совершение этого преступления предусмотрено наказание в виде лишения свободы на срок от 3 до 8 лет.

Часть 2 ст. 635 предусматривает уголовную ответственность за ущерб, причиненный компьютерным системам. Согласно это норме, неуполномоченное лицо, повреждающее или уничтожающее компьютерные системы или программы, компьютерную информацию или данные, подлежит наказанию в виде лишения свободы от 6 месяцев до 3 лет. Если преступление совершено лицом, злоупотребившим правами администратора системы, то срок наказания составляет от 1 до 4 лет лишения свободы.

Испания. Ст. 197 УК Испании предусматривает уголовную ответственность за раскрытие и распространение тайных сведений без согласия их владельца, в том числе сведений из электронной почты и хранящихся в базах данных[1]. Преступлением считаются также перехват телекоммуникаций или использование записывающих и подслушивающих устройств. За совершение этих правонарушений предусмотрено наказание в виде штрафа или заключения на срок от 1 до 4 лет. Если эти данные были разглашены, продемонстрированы или перешли к третьим лицам, санкция увеличивается до лишения свободы на срок от 2 до 5 лет. В ст. 197 есть несколько параграфов, уточняющих наказание в зависимости от тяжести правонарушения; максимальное наказание предусмотрено в случаях, если данные касаются идеологии, религии, здоровья, расы, сексуальной ориентации потерпевшего.

Статьи 198 и 199, связанные со ст. 197, касаются случаев, когда субъектом преступления является лицо, уполномоченное на работу с данными, а также если преступление совершается должностным лицом со злоупотреблением должностными полномочиями. За эти деяния в качестве наказания предусмотрено заключение на срок до 10 лет.

Статья 263 устанавливает ответственность за использование телекоммуникаций без согласия собственника, повлекшее причинение ущерба. Санкция: лишение свободы на срок от 3 месяцев до 1 года.

Часть 2 ст. 264 УК Испании предусматривает ответственность лиц, которые каким-либо образом уничтожат, приведут в негодность или иначе нанесут ущерб чужим электронным данным, программам или документам, находящимся в сети, информационных устройствах или системах. Данное преступление наказывается штрафом или тюремным заключением сроком от 1 до 3 лет.

Ст. 278 УК Испании устанавливает уголовную ответственность за завладение каким-либо способом сведениями, письменными или электронными документами, информационными устройствами или другими объектами, которые относятся к коммерческой тайне.

Великобритания – является страной с системой общего права, ее уголовное законодательство значительно отличается от законодательства других стран Европы.

Компьютерным преступлениям посвящен "Акт о компьютерных злоупотреблениях" 1990 г.[2]

Первый параграф этого Акта касается "неуполномоченного доступа к компьютерным данным". Им установлено, что лицо совершает преступление, когда оно использует компьютер для выполнения любой функции с намерением обеспечить доступ к любой программе или данным, содержащимся в любом компьютере, если этот доступ заведомо неправомочен. Британское уголовное законодательство не делает различия между компьютерами, специально защищенными мерами безопасности и не защищенными.

Кроме того, преступлением признается доступ к компьютеру, с помощью которого изменяются или уничтожаются программы или данные; данные копируются или перемещаются в место, отличное от того, где они содержатся; данные используются (вообще любым способом). За совершение этого преступления предусмотрено наказание в виде штрафа или заключения на срок до 6 месяцев.

Второй параграф Акта о компьютерных злоупотреблениях предусматривает ответственность за "неуполномоченный доступ с намерением совершить другое преступление". Это может быть преступление, предусмотренное Актом, или иное преступление, которое лицо намеревается совершить или облегчить его совершение себе или другому лицу. Наказание, в зависимости от тяжести совершенного деяния, различно – штрафа или лишение свободы до 6 месяцев, а в случае серьезных преступлений – до 5 лет.

Третий параграф Акта посвящен "неуполномоченной модификации компьютерных данных". В соответствии с ним, умышленные действия, влекущие неуполномоченную модификацию содержания любого компьютера, являются преступлением. Для их квалификации следует установить, что модификация содержания являлась целью преступления. Кроме того, лицо должно осознавать, что оно не уполномочено производить модификацию, которую совершает или намеревается совершить. Санкции – те же, что и во втором параграфе.

Нормы об уголовной ответственности за незаконный сбор информации, неправомочный доступ к информации, неправомочный перехват, содержатся также в Акте о регулировании расследований. Он предусматривает, что преднамеренный и без разрешения перехват любой связи в ходе передачи "общественными телекоммуникационными системами" Наказывается штрафом и/или лишением свободы сроком до 2 лет.

Итак, национальное уголовное законодательство европейских государств пока достаточно сильно различается и по объему, и по законодательной технике, и по степени конкретизации деяний.

Что касается сравнения санкций, предусмотренных в разных странах за совершение указанных преступлений то его можно отобразить в табл. 1 и 2.

[1] Ст. 197 Уголовного кодекса Испании 1995г. // Зарубежное законодательство в борьбе с терроризмом. С. 121.

[2] См. подробнее: Решетников Ф.М., Шульженко Н.А. Чрезвычайное законодательство в Великобритании и традиционные институты английского уголовного права // Труды ВНИИСЗ. 23. М., 1982.

Таблица 1

Страна	Незаконный сбор компьютерной информации	Вредоносные программы	Отказ от обслуживания (DNS)	Попытка вторжения
Франция	л/с до 1 года л/с до 5 лет (должностное лицо) штраф	л/с до 2 лет л/с до 3 лет штраф	л/с до 3 лет штраф	л/с до 2 лет штраф
Германия	л/с до 3 лет штраф	л/с до 2 лет л/с до 5 лет (в зависимости от потерпевшего) штраф	л/с до 5 лет штраф	л/с до 3 лет штраф
Италия	л/с до 2 лет штраф	л/с до 3 лет л/с до 4 лет л/с до 5 лет л/с от 3 до 8 лет штраф	л/с от 3 до 8 лет	л/с от 3 лет л/с от 1 до 5 лет
Испания	л/с от 1 до 4 лет штраф	л/с от 1 до 3 лет штраф	л/с от 1 до 3 лет штраф	л/с от 1 до 4 лет штраф
Великобри-тания	л/с до 6 месяцев л/с до 5 лет штраф	штраф л/с от 6 месяцев до 5 лет	Штраф л/с от 6 месяцев до 5 лет	л/с до 6 мес. штраф

Таблица 2

Страна	Неправомочный доступ к информации	Неправомочный перехват	Неправомочная модификация информации	Неправомочный доступ к системам связи
Франция	л/с до 1 года л/с до 2 лет л/с до 5 лет (должностное лицо) штраф	л/с до 1 года л/с до 5 лет (должностное лицо) штраф	л/с до 3 лет штраф	л/с до 2 лет штраф
Германия	л/с до 3 лет штраф	л/с до 3 лет штраф	л/с до 2 лет л/с до 5 лет (в зависимости от потерпевшего) штраф	л/с до 3 лет штраф
Италия	л/с до 2 лет л/с 3 года л/с от 1 до 5 лет штраф	л/с до 2 лет штраф	л/с 3 года л/с от 1 до 5 лет	л/с 3 года л/с от 1 до 5 лет
Испания	л/с от 1 до 4 лет штраф	л/с от 1 до 4 лет штраф	л/с от 1 до 4 лет штраф	л/с от 1 до 4 лет штраф
Великобритания	л/с до 2 лет л/с до 5 лет штраф	л/с до 2 лет штраф	л/с от 6 месяцев до 5 лет штраф	л/с до 2 лет штраф

Как видим, в уголовном законодательстве различных стран предусмотрено достаточно много видов санкций за одно и то же преступление – в зависимости от его тяжести, объекта посягательства, последствий, субъекта преступления и т.п. Разброс степени тяжести наказания достаточно велик. Этот позитивный зарубежный опыт требует внимательного изучения и при необходимости – творческого учета его в законодательстве нашей страны и применении на практике.

Abstract

In the introductory part of the article the author characterizes the influence of information-communicative technologies on development of society.

In the basic part of the article the legislation of European states on provision of information security in cyberspace and struggle with kiberterrorizm are considered.

In the conclusion the author comes to opinion, that it is necessary to study corresponding norms of foreign countries, creatively to make use of their positive experience, and also to unify international norms in the given sphere.

Н.М. Қўшаев
ТДЮИ ўқитувчиси

АЙБ ЭЪЛОН ҚИЛИШ: НАЗАРИЯ, АМАЛИЁТ ВА ҚОНУНЧИЛИК

Муайян шахсга айб элон қилиш жиноят ишларини юритишнинг фақат дастлабки терговда амалга ошириладиган, айбланувчи тариқасида жалб қилинган шахс ва жиноий таъқибни амалга ошираётган давлат органлари ва мансабдор шахсларнинг ўртасида бўладиган процессуал муносабатдир. Айб эълон қилиш шахснинг қандай жиноят содир этганликда айбланаётганлигини расман маълум қилиш ҳисобланади. Айбланувчига айб эълон қилишга, яъни унинг нимада айбланаётганлигини кўрсатишга, ҳимоя ҳуқуқи нуқтаи назаридан зарурат сифатида қаралади.

Шахсга айб эълон қилиш процессуал ҳаракати бир томондан айблов функциясининг амалий кўринишларидан бири деб талқин қилинсада, шахсга нимадан ҳимояланиши кераклигини кўрсатувчи дастур бўлиб хизмат қилади. Қолаверса, шахсни жиноят содир этганликда айбланувчи тариқасида жалб қилишгина эмас, айбловнинг ўз вақтида, кечиктирмасдан эълон қилиниши ҳам ишнинг тўғри, адолатли ва холисона ҳал қилинишида жуда зарур.

Шахсга айб эълон қилиш айбланувчи тариқасида иштирок этишга жалб қилиш яқин тушунчалар ҳисобланади. Чунки айблов эълон қилинишидан аввал жиноят ишидида шахсни айбланувчи тариқасида жалб қилиш тўғрисидаги қарорда ифода этилади.

Жиноят процесси назариясида айб эълон қилиш ва айбланувчи тариқасида жалб қилиш тушунчаларининг ўзаро нисбати масаласи кўплаб илмий мунозаралар сабаб бўлади.

Аксарият процессуалистлар айб эълон қилишни айбланувчи тариқасида жалб қилиш процессуал ҳаракатининг таркибий қисми[1] ёки марказий босқичи[2] деб тушунадилар.

Айрим адабиётларда айб эълон қилиш айбланувчи тариқасиди жалб қилиш билан тенглаштирадилар, айнан бир хил тушунчалар ва процессуал ҳаракатлар деб таъриф берилади[3].

Жиноят содир этгаликда шахсни айбланувчи тариқасида иштирок этишга жалб қилиш фақат шу тўғрисида қарор чиқарилиши билан амалга оширилади, деган фикрни илгари сурадиган олимлар мазкур икки тушунчани бир-биридан айри ва процессда бирин-кетин юз берадиган ҳодисалар деб талқин қиладилар.[4] Бизнингча ҳам айб эълон қилишни шундай тушуниш ўринлидир. Амалдаги жиноят-процессуал қонунчиликда айбланувчи ва гумон қилинувчига берилган таърифлар, дастлабки терговни тўхтатишни тартибга солувчи қоидалар, қолаверса, жиноятлар тергов қилиш амалиёти ҳам айбланувчи тариқасида жалб қилинган ёки айбланувчи деб топилган шахсга айб эълон қилиниши назарда тутади. Яъни икки процессуал ҳаракат турли вақтларда амалга оширилади: олдин шахсни айбланувчи тариқасида иштирок этиш тўғрисида қарор чиқарилади. Унга айбланувчи деган мақом берилади. Шундан кейин айб эълон қилиш, асослар мавжуд бўлганда айбланувчи тариқасида жалб қилинган шахснинг иштироксиз дастлабки терговни тўхтатиш, қидирув эълон қилиш, шу шахсга боғлиқ ҳолатда жиноят ишини тугатиш (мисол учун амнистия актида айбланувчининг шахсини инобатга жавобгарликдан озод қилиш назарда тутилиши мумкин) ва бошқа ҳаракатлар амалга оширилиши мумкин.

Амалдаги жиноят-процессуал қонучилигимизда айб эълон қилиш тартибини белгиловчи қоидалар белгиланмаган. Фақатгина Жиноят-процессуал кодекснинг 552-моддасида "Вояга етмаган шахсга айблов эълон қилиш вақтида ҳимоячи билан бир қаторда вояга етмаган шахснинг қонуний вакили ҳам иштирок этишга ҳақлидир" деган қоида белгилаган, холос.

Терговчилар ўз амалиёт ва тергов анъаларидан келиб чиқиб, мазкур фаолиятни амалга оширмоқдалар. Айбланувчига қарор мазмунини ўқиб бериш ёки айбланувчининг шахсан ўзи танишиб чиқиши учун мазкур қарорни унга тақдим этиш билан айбни эълон қилмоқдалар. Агар айб эълон қилиш ҳимоячининг иштирок этишини талаб қиладиган ҳолларда унинг иштироки

---

[1] Смирнов А.В., Калиновский К.Б. Уголовный процесс: Учебник для вузов / Под общ. ред. А.В. Смирнова. СПб.: Питер, 2004. С.431–432.

[2] Антонов В.Ф. Привлечение в качестве обвиняемого: вопросы теории // Российский следователь. 2006. №8. С.7.

[3].Статкус В.Ф., Цоколов И.А., Жидких А.А. Предъявление обвинения и составление обвинительного заключения / Под ред. И.А. Попова. М.: Книжная находка, 2002. С.12.

[4] В. Божьевнинг фикрича, айб эълон қилиш учун айбланувчи тариқасида жалб қилиш тўғрисида қарор чиқарилади. Қаранг: Божьев В. Предъявление обвинения и допрос обвинямого // Уголовное право. 2001. №2 С.56; А.П. Рыжаковнинг фикрича, шахга айбланувчи мақомини бериш уни айбланувчи тариқасида жалб қилиш тўғрисидаги қарор чиқариш билан якун топади. Айб эълон қилиш эса, айбланувчи тариқасида жалб қилингандан кейинги ҳаракатлардан бири. Қаранг: Обвиняемый: понятие, права и обязанности: Научно-практическое руководство / Рыжаков А.П. Ростов н/Д.: Феникс, 2006. С.8–9.