П О С Т А Н О В Л Е Н И Е

Парламентской Ассамблеи
Организации Договора о коллективной безопасности

О проекте Рекомендательного перечня
составов преступлений и административных правонарушений
в сфере обеспечения информационной безопасности личности, общества
и государства для государств – членов ОДКБ

Парламентская Ассамблея Организации Договора о коллективной безопасности п о с т а н о в л я е т:

1. Принять Рекомендательный перечень составов преступлений и административных правонарушений в сфере обеспечения информационной безопасности личности, общества и государства для государств – членов ОДКБ (далее – Рекомендательный перечень) (прилагается).

2. Направить указанный в пункте 1 настоящего постановления Рекомендательный перечень в парламенты государств – членов ОДКБ для использования в работе по совершенствованию законодательства государств – членов Организации в соответствующей сфере.

3. Разместить Рекомендательный перечень на официальном сайте и опубликовать в печатных материалах Парламентской Ассамблеи ОДКБ.

Председатель
Парламентской Ассамблеи ОДКБ **В.В.ВОЛОДИН**

Ереван
5 ноября 2019 года
№ 12-4.2

Принят
на двенадцатом пленарном заседании
Парламентской Ассамблеи ОДКБ
5 ноября 2019 года, постановление № 12-4.2

РЕКОМЕНДАТЕЛЬНЫЙ ПЕРЕЧЕНЬ
составов преступлений и административных правонарушений в сфере обеспечения информационной безопасности личности, общества и государства для государств – членов ОДКБ

Проблема гармонизации деликтного законодательства в государствах – членах ОДКБ поднималась на разных уровнях и неоднократно. В частности, в 2017 году были приняты Рекомендации по совершенствованию уголовного законодательства государств – членов ОДКБ по вопросам борьбы с правонарушениями в информационной сфере (постановление Парламентской Ассамблеи ОДКБ от 13 октября 2017 года № 10-3.8). Данные Рекомендации затрагивают вопросы уголовно-правовой и административно-деликтной защиты государственно значимой информации. Проблемы обеспечения правовой защиты коммерческой тайны, персональных данных и иной защищаемой на законодательном уровне информации в силу разнородности их регулирования в законодательстве государств – членов ОДКБ требуют разработки отдельных рекомендаций.

В настоящий период, в условиях нарастающей цифровизации многих экономических и иных общественных отношений, резкого увеличения возможностей для анализа сведений, циркулирующих и хранящихся в Интернете, многочисленных системах компьютерных коммуникаций, именуемых «социальными сетями», возникает необходимость в поиске новых путей юридической защиты личности, общества и государства от противоправных посягательств в этой сфере. Как представляется, данная работа имеет пролонгированный характер, что обусловлено, в первую очередь, с появлением новых конкретных угроз в сфере обеспечения информационной безопасности, а также развитием законодательства государств – членов ОДКБ в области государственного управления, в области информатизации, в области развития цифровой экономики и иных областях, связанных с информационным обменом.

На первом этапе, который представлен данным Рекомендательным перечнем, решается, в основном, задача упорядочения имеющихся составов преступлений и административных правонарушений, обеспечивающих правовую защиту отношений в области оборота сведений ограниченного доступа и информации, хранимой в машиночитаемом виде (компьютерной информации).

Уголовно-правовая и административно-правовая защита сведений, составляющих государственную тайну (государственные секреты)

Республика Армения, Кыргызская Республика, Российская Федерация и Республика Таджикистан используют в своем деликтном законодательстве такое системное понятие, как государственная тайна. В Республике Беларусь и Республике Казахстан используется понятие «государственные секреты», составной частью которого является государственная тайна. Постановлением Парламентской Ассамблеи Организации Договора о коллективной безопасности от 13 октября 2017 года № 10-3.1 был принят модельный закон ОДКБ «О государственной тайне».

В связи с этим в конструируемых модельных нормах будет использоваться понятие «государственная тайна».

С учетом того, что установление конкретного наказания за совершенное деяние является исключительной прерогативой любого суверенного государства, в конструируемых модельных нормах опущены санкции за описанные деяния.

1. Государственная измена (измена государству)

Проведенный анализ показал, что наиболее совершенным с точки зрения вложенного юридического смысла и охвата общественных отношений является описание данного деяния, содержащееся в Уголовном кодексе Республики Беларусь. Взятое за основу описание объективной стороны преступления, предусмотренного статьей 356 УК данного государства, предлагается в качестве конструируемой модельной нормы в следующем виде:

«Государственная измена, то есть выдача гражданином… иностранному государству, международной либо иностранной организации или их представителям доверенных ему сведений, составляющих государственную тайну, а равно доверенных ему сведений, составляющих государственную тайну иного государства, переданных *(название государства)* в соответствии с международным договором, либо шпионаж, либо переход на сторону врага во время войны или вооруженного конфликта, либо оказание финансовой, материально-технической, консультационной или иной помощи иностранному государству, международной либо иностранной организации или их представителям в деятельности, направленной на причинение ущерба национальной безопасности *(название государства)*, –

наказывается…

Примечание. Лицо, совершившее преступления, предусмотренные настоящей статьей, за исключением перехода на сторону врага во время войны или вооруженного конфликта, освобождается от уголовной ответственности, если оно добровольным и своевременным сообщением органам власти или иным образом способствовало предотвращению дальнейшего ущерба национальной безопасности *(название государства)*, и если в его действиях не содержится иного состава преступления».

С учетом тяжести данного деяния и его однозначной принадлежности по степени общественной опасности к сфере уголовного законодательства корреспондирующие ему административно-деликтные нормы не формулируются.

2. Шпионаж

В связи с тем, что состав преступления, получивший в уголовном законодательстве государств – членов ОДКБ название «шпионаж», в том случае, если он совершен гражданином одного из этих государств, признается государственной изменой, он терминологически и категориально должен быть связан с описанием этого деяния и тогда, когда это преступление совершается иностранным гражданином или лицом без гражданства. На основании этого предлагается следующая формулировка диспозиции данной уголовно-правовой нормы:

«Шпионаж, то есть собирание, похищение или хранение с целью передачи иностранному государству, международной или иностранной организации либо их представителям сведений, составляющих государственную тайну *(название государства)*, а равно сведений, составляющих государственную тайну иного государства, переданных *(название государства)* в соответствии с международным договором, а также собирание, похищение или хранение с целью передачи по заданию иностранной разведки, организации или лица, действующих в ее интересах, иных сведений с целью причинения ущерба национальной безопасности *(название государства)*, если эти деяния совершены иностранным гражданином или лицом без гражданства, –

наказывается…

Примечание. Лицо, совершившее преступления, предусмотренные настоящей статьей, освобождается от уголовной ответственности, если оно добровольным и своевременным сообщением органам власти… или иным образом способствовало предотвращению дальнейшего ущерба национальной безопасности *(название государства)* и если в его действиях не содержится иного состава преступления».

С учетом тяжести данного деяния и его однозначной принадлежности по степени общественной опасности к сфере уголовного законодательства корреспондирующие ему административно-деликтные нормы не формулируются.

3. Разглашение государственной тайны и утрата носителей таких сведений

Категория «разглашение» используется уголовным законодательством всех государств – членов ОДКБ либо в качестве системного понятия (Республика Армения, Республика Беларусь, Кыргызская Республика, Российская Федерация, Республика Таджикистан), либо в качестве одного из

видов деяния, связанного с распространением такого рода информации (Республика Казахстан).

С учетом важности данного понятия для описания противоправного деяния, представляется необходимым определить его лингвистическую составляющую. Толковые словари русского языка определяют производность этого слова от глаголов «разгласить», «разглашать», которые означают действие, заключающееся в том, что информация становится известной всем, повсюду, причем делается акцент на негативности данного действия. Таким образом, понятия «разглашение» и «распространение» для целей формулирования юридических норм деликтной направленности можно воспринимать в качестве синонимов. Однако, как представляется, это не совсем правильно. Категорию «разглашение» следует употреблять в том случае, если речь идет об умышленном деянии. Когда же речь идет о неосторожном деянии, в целях лингвистического его отграничения от умышленного деяния следует употреблять категорию «распространение».

При продолжении данного логического рассуждения получается, что сообщение информации неуправомоченному лицу (третьему лицу) нельзя квалифицировать как разглашение, так как в данном случае она не становится доступной неопределенному кругу лиц. Если в этом случае не произошло дальнейшего распространения сведений, то наказание должно быть установлено на более низком уровне. Формулирование отдельной диспозиции уголовно-правовой нормы в этом случае не требуется, так как современное уголовное законодательство содержит достаточное количество способов смягчения наказания в рамках одного состава преступления.

На основании анализа соответствующих составов преступлений, содержащихся в уголовном законодательстве государств – членов ОДКБ, и вышеизложенных рассуждений предлагаются следующие формулировки диспозиций уголовно-правовых норм:

1) «1. Разглашение, то есть сообщение неопределенному кругу лиц сведений, составляющих государственную тайну, лицом, которому они стали известны в связи с исполнением служебных, трудовых обязанностей либо по иным предусмотренным законодательством *(название государства)* основаниям, при отсутствии признаков государственной измены или шпионажа, –

наказывается…

2. То же деяние, повлекшее за собой тяжкие последствия, –

наказывается…»;

2) «1. Разглашение, то есть сообщение неопределенному кругу лиц сведений, составляющих государственную тайну, лицом, которому они стали известны в связи с исполнением служебных, трудовых обязанностей либо по иным предусмотренным – законодательством *(название государства)* основаниям, по неосторожности, –

наказывается…

2. То же деяние, повлекшее за собой тяжкие последствия, –

наказывается…»;

3) «1. Сообщение неуправомоченному лицу (лицам) сведений, составляющих государственную тайну, при условии, что не было допущено их разглашение неопределенному кругу лиц, при отсутствии признаков государственной измены или шпионажа, –

наказывается…

2. То же деяние, повлекшее за собой тяжкие последствия, –

наказывается…

Примечание. Лицо, совершившее преступление, предусмотренное частью первой настоящей статьи, освобождается от уголовной ответственности, если оно добровольным и своевременным сообщением органам власти *(название государства)* или иным образом способствовало предотвращению дальнейшего ущерба национальной безопасности *(название государства)* и если в его действиях не содержится иного состава преступления»;

4) «1. Предоставление неуправомоченному лицу (лицам) возможности доступа к сведениям, составляющим государственную тайну, содержащимся в базе (банке) данных компьютерной информации, путем сообщения пароля доступа или предоставления иных средств идентификации пользователя этой базой (банком) данных, –

наказывается…

2. То же деяние, если оно повлекло за собой разглашение сведений, составляющих государственную тайну, –

наказывается…

3. То же деяние, если оно повлекло за собой тяжкие последствия, –

наказывается…».

Некоторой модификации с целью уточнения сущности преступного деяния должно быть подвергнуто и описание уголовно наказуемого деяния, связанного с носителями информации, составляющей государственную тайну. В уголовном законодательстве государств – членов ОДКБ состав преступления, связанного с утратой документов, содержащих государственную тайну, ориентирован в основном только на документы, отображаемые на бумажных носителях, тогда как все более массовый характер приобретает хранение такой информации на иных носителях (оптические диски, внешние жесткие диски, флеш-накопители и т. д.). В частности, это практически полностью касается хранения составляющих государственную тайну цифровых фотоснимков и видеозаписей, причем не во всех случаях такие файлы имеют статус официальных документов в том смысле, который придают документам соответствующие государственные стандарты.

В связи с указанным предлагается следующее описание уголовно наказуемого деяния:

«Утрата сведений, составляющих государственную тайну

Нарушение лицом, в служебные или трудовые обязанности которого входит соблюдение установленных правил обращения со сведениями, составляющими государственную тайну, указанных правил, если это по неосторожности повлекло за собой утрату носителей информации, содержащих такие сведения, и наступление тяжких последствий, –

наказывается…».

Данному перечню составов преступлений должен корреспондировать определенный перечень административных правонарушений, так как некоторые из вышеописанных деяний в случае, если они не образуют состава преступления, по своей сущности остаются юридическими деликтами.

Для этих целей предлагаются следующие формулировки видов административных правонарушений:

1) «Сообщение неуправомоченному лицу (лицам) сведений, составляющих государственную тайну, если эти действия не содержат уголовно наказуемого деяния, –

влечет за собой наложение…»;

2) «Хранение паролей доступа или иных средств идентификации пользователя баз (банков) данных, содержащих сведения, составляющие государственную тайну, в условиях, когда не исключена возможность доступа к ним постороннего лица (лиц), –

влечет за собой наложение…»;

3) «Нарушение лицом, в служебные или трудовые обязанности которого входит соблюдение установленных правил обращения со сведениями, составляющими государственную тайну, указанных правил, если при этом возникли реальные предпосылки к утрате носителей информации, содержащих сведения, составляющие государственную тайну, –

влечет за собой наложение…

То же деяние, по неосторожности повлекшее за собой утрату носителей информации, содержащих такие сведения, если эти действия не содержат уголовно наказуемого деяния, –

влечет за собой наложение…».

4. Правонарушения в сфере оборота и защиты сведений, обрабатываемых и хранящихся в автоматизированных (компьютерных) системах

4.1. Противоправный доступ к сведениям, обрабатываемым и хранящимся в автоматизированных (компьютерных) системах

Уголовное законодательство государств – членов ОДКБ по-разному трактует информацию, которая находится в компьютерных системах: компьютерная информация; информация, хранящаяся в компьютерной системе;

информация, содержащаяся в информационной системе. В связи с этим требуется определенная унификация данных понятий, которая отражала бы суть охраняемых уголовным законодательством отношений.

Помимо вышеназванных, разной степенью общественной опасности обладают такие действия, как изменение содержания хранимых в автоматизированной системе сведений и изменение программного обеспечения данной автоматизированной системы, хотя в настоящее время все это охватывается термином «модификация информации» и с уголовно-правовой точки зрения не различается. Как представляется, умышленное изменение программного обеспечения для преодоления рубежей защиты и дальнейшего управления функционированием автоматизированной системы в противоправных целях является наиболее общественно опасным из всех уголовно наказуемых деяний, так как может повлечь за собой тяжкие последствия, например, при работе транспорта, трубопроводных систем, которые приведут к человеческим жертвам или к экологическому ущербу.

На основании сказанного предлагаются следующие описания уголовно наказуемых деяний:

1) «Противоправный доступ к охраняемой законом информации, находящейся в отдельном компьютере, автоматизированной информационной системе, компьютерной сети или на отдельных носителях такой информации, сопровождающийся нарушением системы ее защиты, если это создало угрозу наступления тяжких последствий, –

наказывается…»;

2) «Противоправное уничтожение или блокирование охраняемой законом информации

1. Противоправное уничтожение или блокирование охраняемой законом информации, хранящейся на отдельном компьютере, в автоматизированной информационной системе или передаваемой по компьютерным сетям, если это создало угрозу наступления тяжких последствий, –

наказывается…

2. То же деяние, совершенное с целью воздействия на критическую информационную инфраструктуру *(название государства)* или повлекшее за собой тяжкие последствия, а равно совершенное по предварительному сговору или организованной группой лиц, –

наказывается…»;

3) «Противоправное внесение изменений в программное обеспечение

1. Противоправное внесение изменений в программное обеспечение отдельного компьютера, автоматизированной информационной системы или компьютерной сети, которое привело к нарушениям в ее работе и создало угрозу наступления тяжких последствий, –

наказывается…

2. То же деяние, повлекшее за собой наступление тяжких последствий, а равно совершенное по предварительному сговору или организованной группой лиц, –

наказывается…».

Данным уголовно наказуемым деяниям, как представляется, должно корреспондировать административное правонарушение со следующим описанием:

«Противоправные действия в отношении информации, содержащейся в компьютерах и автоматизированных информационных системах

Противоправные доступ, уничтожение или блокирование охраняемой законом информации, хранящейся на отдельном компьютере, в автоматизированной информационной системе или передаваемой по компьютерным сетям, а равно противоправное внесение изменений в программное обеспечение автоматизированной информационной системы или компьютерной сети, которое привело к нарушениям в ее работе, если эти действия не содержат уголовно наказуемого деяния, –

влечет за собой наложение…».

4.2. Создание, использование и распространение вредоносных программ для ЭВМ (компьютерных программ)

Разработка программ, специально предназначенных для того, чтобы вносить дезорганизацию в программное обеспечение различных автоматизированных систем, заставлять их работать не по первоначально определенному алгоритму, похищать или уничтожать определенную информацию, осуществлять иные действия, препятствующие нормальной работе отдельных компьютеров или их систем, в настоящее время превратилась в своего рода «индустрию». Объем так называемых вирусных программ, «троянских коней» и прочего постоянно нарастает, они совершенствуются и становятся более опасными в связи с тем, что, во-первых, автоматизация различных процессов в промышленности и государственном управлении непрерывно расширяется, а, во-вторых, программы такого предназначения стали оружием, то есть их разработку осуществляют не только группы «энтузиастов», но и государственные структуры отдельных стран, в силу чего на рынке труда появляются высококлассные специалисты, способные разработать весьма опасные для мировой телекоммуникационной среды вредоносные программы.

Однако не во всех случаях речь должна идти исключительно о разработке новых программ. Распространены случаи, когда видоизменение существующих программ наделяет их свойствами вредоносности, что также должно учитываться уголовным законодательством.

Помимо указанного, весьма полемично выглядит категория «иная компьютерная информация» в контексте ее вредоносности, которая использована в диспозиции статьи 273 Уголовного кодекса Российской Федерации – «Создание, использование и распространение вредоносных компьютерных программ». Дело в том, что компьютерная программа по своей сущности есть комбинация компьютерных инструкций (совокупность команд) и данных (поддающейся многократной интерпретации информации в формализованном виде, пригодном для передачи, связи или обработки). При этом следует полагать, что система команд первична по отношению к данным. Следовательно, вредоносная программа прежде всего является системой команд.

При анализе уголовного законодательства государств – членов ОДКБ также выявилось, что все они, за исключением законодательства Республики Казахстан, при описании уголовно наказуемого деяния, связанного с вредоносными программами, оперируют данной категорией во множественном числе, что неправильно, так как уголовное наказание должно следовать не только за создание, распространение или использование некоего множества программ, но и за указанные действия в отношении одной вредоносной программы.

На основании вышеизложенного конструируемое описание преступления можно представить в следующем виде:

«1. Создание компьютерной программы или внесение изменений в существующую компьютерную программу, заведомо предназначенных для противоправного уничтожения, блокирования, модификации, копирования компьютерной информации, нарушения работы отдельного компьютера, автоматизированной информационной системы, компьютерной сети или нейтрализации средств их защиты, –

наказывается...

2. То же деяние, совершенное с целью воздействия на критическую информационную инфраструктуру *(название государства)* либо повлекшее за собой наступление тяжких последствий, а равно совершенное по предварительному сговору или организованной группой лиц, –

наказывается…».

Данному уголовно наказуемому деянию, как представляется, должно корреспондировать следующее административное правонарушение:

«Создание компьютерной программы или внесение изменений в существующую компьютерную программу, использование которых по неосторожности привело к противоправному уничтожению, блокированию, модификации, копированию компьютерной информации, нарушению работы отдельного компьютера, автоматизированной информационной системы, компьютерной сети или нейтрализации средств их защиты и тем самым причинило материальный ущерб, если эти действия не содержат уголовно наказуемого деяния, –

влечет за собой наложение…».

4.3. Нарушение правил эксплуатации компьютеров, автоматизированных информационных систем и компьютерных сетей

Существенно различаются между собой в уголовных законах государств – членов ОДКБ и описания преступных деяний, связанных с нарушением установленных правил эксплуатации отдельных компьютеров и компьютерных систем. Такого рода правонарушения в настоящее время приобретают все большую общественную опасность в силу дальнейшей автоматизации самых различных процессов, создания автоматизированных банков данных, перевода на компьютерные технологии управления транспортом, экологически опасными промышленными производствами, управления оружием и боевой техникой.

В этом случае терминологическая унификация в описании уголовно наказуемого деяния тоже имеет существенное значение для государств – членов ОДКБ, так как способствует сближению уголовно-правовой политики в борьбе с данными общественно опасными деяниями.

Прежде всего обращает на себя внимание терминологическое разнообразие объектов, нарушение правил эксплуатации которых является уголовно наказуемым. В Уголовном кодексе Российской Федерации ими являются средства хранения, обработки или передачи охраняемой компьютерной информации, информационно-телекоммуникационные сети и оконечное оборудование, а также деликты, связанные с нарушением правил доступа к указанным объектам, повлекшие за собой крупный ущерб или иные негативные последствия. В Уголовном кодексе Республики Армения это компьютер, компьютерные системы или сети. В Уголовном кодексе Республики Беларусь и Уголовном кодексе Республики Таджикистан в таком качестве выступают компьютерные системы или сети, а в Уголовном кодексе Республики Казахстан – информационные сети и сети телекоммуникаций. Уголовное законодательство Кыргызской Республики по-прежнему не предусматривает наказания за такого рода деяния.

В связи с указанным целесообразно опереться на приведенный выше универсальный перечень таких объектов и сделать акцент на легальности правил эксплуатации.

Конструируемое описание преступления можно представить в следующем виде:

«1. Нарушение нормативно установленных правил эксплуатации отдельного компьютера, автоматизированной информационной системы, компьютерной сети или средств их защиты, а также нормативно установленных правил доступа к автоматизированным информационным системам или сетям, повлекшее нарушение их работы, а равно уничтожение, блокирование, модификацию либо копирование хранимой и обрабатываемой в них информации, причинившее крупный ущерб, –

наказывается...

2. То же деяние, совершенное с целью воздействия на критическую информационную инфраструктуру *(название государства)* либо повлекшее за собой наступление тяжких последствий, а равно совершенное по предварительному сговору или организованной группой лиц, –

наказывается…».

Как представляется, данному уголовно наказуемому деянию должно корреспондировать следующее административное правонарушение:

«Нарушение нормативно установленных правил эксплуатации отдельного компьютера, автоматизированной информационной системы, компьютерной сети или средств их защиты, а также нормативно установленных правил доступа к автоматизированным информационным системам или сетям, повлекшее нарушение их работы, а равно уничтожение, блокирование, модификацию либо копирование хранимой и обрабатываемой в них информации, причинившее крупный ущерб, если эти действия не содержат уголовно наказуемого деяния, –

влечет за собой наложение…».