РЕКОМЕНДАЦИИ
по сближению и гармонизации уголовного и административно-деликтного законодательства государств – членов ОДКБ в области безопасности критической информационной инфраструктуры

Введение

Процесс цифровизации в различных сферах жизнедеятельности государства и общества во всех государствах – членах ОДКБ идет нарастающими темпами. Эти вопросы находят отражение и в деятельности Парламентской Ассамблеи Организации Договора о коллективной безопасности. 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), в 2019 году был принят Рекомендательный перечень составов преступлений и административных правонарушений в сфере обеспечения информационной безопасности личности, общества и государства для государств – членов ОДКБ (постановление Парламентской Ассамблеи ОДКБ от 5 ноября 2019 года № 12-4.2).

Одной из важных составляющих данного процесса в настоящее время является автоматизация и цифровизация в области управления промышленными объектами, объектами энергетики, связи, транспорта и иными, которые принято обобщенно именовать объектами критической информационной инфраструктуры. 19 декабря 2023 года постановлением Парламентской Ассамблеи Организации Договора о коллективной безопасности № 16-6.1 был принят модельный закон ОДКБ «О безопасности критической информационной инфраструктуры». Действенность его регулятивных норм в случае их имплементации в национальном законодательстве государств – членов ОДКБ невозможно обеспечить без формулирования адекватных охранительных норм. Модель решения этой правовой проблемы представлена в настоящих Рекомендациях.

Раздел I. Рекомендации по совершенствованию уголовного законодательства государств – членов ОДКБ по вопросам борьбы с преступлениями в сфере обеспечения защиты критической информационной инфраструктуры

Все действующие в настоящее время уголовные законы государств – членов ОДКБ имеют в структуре своих особенных частей главы, связанные с описанием преступлений в области компьютерной безопасности, кибербезопасности, сфере информатизации и связи либо информационной безопасности.

Соответствующие положения уголовных законов государств – членов ОДКБ характеризуются следующим образом.

Республика Армения

В Особенной части Уголовного кодекса Республики Армения имеется глава 38 «Преступления против безопасности компьютерной системы и компьютерной информации», в рамках которой объединено семь статей. Ни один из сформулированных в них составов преступлений не касается уголовно-правовой защиты отношений в области обеспечения безопасности критической информационной инфраструктуры.

Республика Беларусь

В Особенной части Уголовного кодекса Республики Беларусь имеется глава 31 «Преступления против компьютерной безопасности», в рамках которой объединено пять статей. Ни один из сформулированных в них составов преступлений не касается уголовно-правовой защиты отношений в области обеспечения безопасности критической информационной инфраструктуры.

Республика Казахстан

Особенная часть Уголовного кодекса Республики Казахстан содержит главу 7 «Уголовные правонарушения в сфере информатизации и связи», которая объединяет шесть статей.

Статья 205 «Неправомерный доступ к информации, в информационную систему или сеть телекоммуникаций» имеет квалифицированный состав (часть 2), увеличивающий уголовную санкцию за то же деяние, совершенное в отношении критически важных объектов информационно-телекоммуникационной инфраструктуры.

Статья 206 «Неправомерные уничтожение или модификация информации» имеет квалифицированный состав (пункт 1 части 2), увеличивающий уголовную санкцию за то же деяние, совершенное в отношении критически важных объектов информационно-коммуникационной инфраструктуры.

Статья 207 «Нарушение работы информационной системы или сетей телекоммуникаций» имеет квалифицированный состав (пункт 1 части 2), увеличивающий уголовную санкцию за то же деяние, совершенное в отношении критически важных объектов информационно-коммуникационной инфраструктуры.

Статья 208 «Неправомерное завладение информацией» имеет квалифицированный состав (пункт 1 части 2), увеличивающий санкцию за то же деяние, совершенное в отношении критически важных объектов информационно-коммуникационной инфраструктуры.

Статья 209 «Принуждение к передаче информации» имеет квалифицированный состав (пункт 3 части 2), увеличивающий уголовную

санкцию за то же деяние, совершенное с целью получения информации из критически важных объектов информационно-коммуникационной инфраструктуры.

Статья 210 «Создание, использование или распространение вредоносных компьютерных программ и программных продуктов» имеет квалифицированный состав (пункт 3 части 2), увеличивающий уголовную санкцию за то же деяние, совершенное в отношении критически важных объектов информационно-коммуникационной инфраструктуры.

Кыргызская Республика

В Особенной части Уголовного кодекса Кыргызской Республики содержится глава 40 «Преступления против кибербезопасности», в рамках которой объединены четыре статьи. Две из них имеют составы, связанные с обеспечением безопасности критической информационной инфраструктуры.

Статья 319 «Несанкционированный доступ к компьютерной информации и электронным документам, в информационную систему или сеть электросвязи» содержит квалифицированный состав, увеличивающий уголовную санкцию за то же деяние (пункт 3 части 2), совершенное в отношении информационных систем или сетей электросвязи, относящихся к критической информационной инфраструктуре.

Помимо указанного, если данное деяние совершено с целью умышленного уничтожения, изменения, блокирования, приведения в непригодное состояние компьютерной информации или электронного документа либо вывода из строя, разрушения информационных систем или сети электросвязи, его совершение в отношении информационных систем или сетей электросвязи, относящихся к критической информационной инфраструктуре, также предусматривает повышенный уровень уголовной ответственности.

Статья 320 «Создание вредоносных программных продуктов» содержит квалифицированный состав, увеличивающий уголовную санкцию за то же деяние (пункт 3 части 2), совершенное в отношении информационных систем или сетей электросвязи, относящихся к критической информационной инфраструктуре.

Российская Федерация

В Особенной части Уголовного кодекса Российской Федерации содержится глава 28 «Преступления в сфере компьютерной информации», в рамках которой объединено пять статей, две из них имеют составы, направленные на обеспечение уголовно-правовой защиты критической информационной инфраструктуры.

Статья 274.1 «Неправомерное воздействие на критическую информационную инфраструктуру Российской Федерации» содержит три состава преступления, связанные с критической информационной инфраструктурой.

1. Создание, распространение и (или) использование компьютерных программ либо иной компьютерной информации, заведомо предназначенных для неправомерного воздействия на критическую информационную инфраструктуру Российской Федерации, в том числе для уничтожения, блокирования, модификации, копирования информации, содержащейся в ней, или нейтрализации средств защиты указанной информации.

Данное деяние сходно с диспозицией статьи 273 Уголовного кодекса Российской Федерации «Создание, использование и распространение вредоносных компьютерных программ», однако в нем специально выделяется отграничивающий признак противоправного воздействия на критическую информационную инфраструктуру, что влечет за собой увеличение предельных значений уголовно-правовых санкций по сравнению с аналогичным составом статьи 273 Уголовного кодекса Российской Федерации.

2. Неправомерный доступ к охраняемой компьютерной информации, содержащейся в критической информационной инфраструктуре Российской Федерации, в том числе с использованием компьютерных программ либо иной компьютерной информации, которые заведомо предназначены для неправомерного воздействия на критическую информационную инфраструктуру Российской Федерации, или иных вредоносных компьютерных программ, если он повлек причинение вреда критической информационной инфраструктуре Российской Федерации.

Данное деяние в некоторой степени сходно с диспозицией статьи 272 Уголовного кодекса Российской Федерации «Неправомерный доступ к компьютерной информации», однако в нем содержится ряд важных дополнений, связанных с критической информационной инфраструктурой, в том числе акцент на причинение вреда такого рода охраняемым объектам. Совершение деяния, подпадающего под данные признаки, также влечет за собой увеличение предельных значений уголовно-правовых санкций по сравнению с аналогичным составом статьи 272 Уголовного кодекса Российской Федерации.

3. Нарушение правил эксплуатации средств хранения, обработки или передачи охраняемой компьютерной информации, содержащейся в критической информационной инфраструктуре Российской Федерации, или информационных систем, информационно-телекоммуникационных сетей, автоматизированных систем управления, сетей электросвязи, относящихся к критической информационной инфраструктуре Российской Федерации, либо правил доступа к указанным информации, информационным системам, информационно-телекоммуникационным сетям, автоматизированным системам управления, сетям электросвязи, если оно повлекло причинение вреда критической информационной инфраструктуре Российской Федерации.

Данное деяние в некоторой степени сходно с диспозицией статьи 274 Уголовного кодекса Российской Федерации, однако содержит ряд существенных дополнений, связанных с видами объектов критической

информационной инфраструктуры. Привлечение к уголовной ответственности за деяние, предусмотренное частью первой статьи 274 Уголовного кодекса Российской Федерации возможно только при причинении крупного ущерба. В рассматриваемой норме ответственность наступает при причинении ущерба без каких-либо дополнительных признаков.

Совершение данного деяния, как и в вышеуказанных случаях, влечет за собой по сравнению со статьей 274 Уголовного кодекса Российской Федерации более жесткое уголовное наказание.

В соответствии с принятой в российском уголовном законодательстве градацией квалификации преступных деяний по уровням при совершении вышеуказанных преступлений группой лиц по предварительному сговору, организованной группой, лицом с использованием своего служебного положения, а также при возникновении тяжких последствий уголовные санкции существенно ужесточаются.

Следующим блоком уголовно наказуемых деяний, имеющих направленность на обеспечение правовой защиты отношений в области критической информационной инфраструктуры, является статья 274.2 «Нарушение правил централизованного управления техническими средствами противодействия угрозам устойчивости, безопасности и целостности функционирования на территории Российской Федерации информационно-телекоммуникационной сети «Интернет» и сети связи общего пользования».

В данной статье сформулированы два состава преступлений, обеспечивающие уголовно-правовую защиту в этой области общественных отношений.

1. Нарушение порядка установки, эксплуатации и модернизации в сети связи технических средств противодействия угрозам устойчивости, безопасности и целостности функционирования на территории Российской Федерации информационно-телекоммуникационной сети «Интернет» и сети связи общего пользования либо несоблюдение технических условий их установки или требований к сетям связи при использовании указанных технических средств, совершенные должностным лицом или индивидуальным предпринимателем, подвергнутыми административному наказанию за деяние, предусмотренное частью 2 статьи 13.42 Кодекса Российской Федерации об административных правонарушениях.

2. Нарушение требований к пропуску трафика через технические средства противодействия угрозам устойчивости, безопасности и целостности функционирования на территории Российской Федерации информационно-телекоммуникационной сети «Интернет» и сети связи общего пользования, совершенное должностным лицом или индивидуальным предпринимателем, подвергнутыми административному наказанию за деяние, предусмотренное частью 2 статьи 13.42.1 Кодекса Российской Федерации об административных правонарушениях.

Важность установки и эксплуатации таких систем не вызывает сомнений, так как информационно-телекоммуникационная сеть «Интернет» в

настоящее время стала одной из самых эксплуатируемых систем коммуникаций между гражданами и организациями, от бесперебойности и безопасности функционирования которой зависит деятельность и органов публичной власти, и огромного числа организаций, в том числе связанных с безопасностью населения и оказанием срочной помощи гражданам.

Характерным для приведенных выше составов преступлений является то, что уголовная ответственность по ним возникает только в случае, если лицо ранее привлекалось к административной ответственности за сходные деяния (реализация доктрины повышения уровня ответственности за повторность).

Республика Таджикистан

В Особенной части Уголовного кодекса Республики Таджикистан имеется глава 28 «Преступления против информационной безопасности», в рамках которой объединено семь статей. Ни один из сформулированных в них составов преступлений не касается уголовно-правовой защиты отношений в области обеспечения безопасности критической информационной инфраструктуры.

Анализ показывает, что не во всех государствах – членах ОДКБ предусмотрена уголовная ответственность за преступления, имеющие направленность на причинение вреда критической информационной инфраструктуре. При этом просматриваются два подхода:

1) установление более высокого уровня наказаний за уже предусмотренные уголовными законами преступления в случае их совершения в отношении объектов критической информационной инфраструктуры (Республика Казахстан, Кыргызская Республика);

2) введение в уголовный закон новых составов преступлений, имеющее своей целью уголовно-правовую защиту отношений в области обеспечения безопасности критической информационной инфраструктуры (Российская Федерация).

Следует признать оба подхода равнозначными и вполне отвечающими своим задачам. Возможна также реализация третьего, интегрированного подхода, когда в рамках одной статьи формулируется новый состав преступления и при этом имеющаяся структура уголовного закона в части нумерации статей остается прежней.

С учетом важности правовой защиты отношений в области обеспечения безопасности критической информационной инфраструктуры целесообразно предложить законодателям Республики Армения, Республики Беларусь и Республики Таджикистан установить уголовную ответственность за деяния, связанные с посягательством на безопасность такой инфраструктуры.

Раздел II. Рекомендации по совершенствованию административно-деликтного законодательства государств – членов ОДКБ по вопросам борьбы с правонарушениями в сфере обеспечения защиты критической информационной инфраструктуры

Защита отношений, связанных с обеспечением безопасности критической информационной инфраструктуры, посредством административно-деликтных норм, является весьма важной правовой задачей, так как позволяет существенно расширить зону юридической защиты деятельности такого рода объектов. Это связано с возможностью значительно более упрощенного порядка привлечения к административной ответственности, применения более мягких мер, а также изменения направленности юридической ответственности от карательной функции к карательно-стимулирующей, то есть имеющей задачу не только наказания за содеянное, но и улучшения деятельности объекта в случае привлечения к ответственности должностных лиц или юридических лиц.

Также следует отметить, что уголовной ответственности во всех государствах – членах ОДКБ, за исключением Республики Армения, подлежат только физические лица. Законодательство об административных правонарушениях, действующее во всех государствах – членах ОДКБ, позволяет привлекать к деликтной ответственности и юридических лиц, что делает возможным более широкое использование административно-деликтного законодательства для защиты отношений в области обеспечения безопасности критической информационной инфраструктуры.

Республика Армения

Административно-деликтные нормы, касающиеся обеспечения безопасности критической информационной инфраструктуры, в Кодексе Республики Армения об административных правонарушениях отсутствуют.

Республика Беларусь

Административно-деликтные нормы, касающиеся обеспечения безопасности критической информационной инфраструктуры, в Кодексе Республики Беларусь об административных правонарушениях отсутствуют.

Республика Казахстан

В Кодексе Республики Казахстан об административных правонарушениях имеется статья 641 «Нарушение законодательства Республики Казахстан об информатизации», часть пятая которой содержит описание следующего административного правонарушения:

«Неоповещение собственником или владельцем критически важных объектов информационно-коммуникационной инфраструктуры Национального координационного центра информационной безопасности об инцидентах информационной безопасности и о результатах реагирования на

них в порядке и сроки, которые определены правилами проведения мониторинга обеспечения информационной безопасности объектов информатизации «электронного правительства» и критически важных объектов информационно-коммуникационной инфраструктуры, если иное не установлено законодательными актами Республики Казахстан…»

Частью шестой той же статьи установлены повышенные меры административной ответственности в случае совершения указанных правонарушений повторно в течение года после наложения административного взыскания.

Кыргызская Республика

Административно-деликтные нормы, касающиеся обеспечения безопасности критической информационной инфраструктуры, в Кодексе Кыргызской Республики о правонарушениях отсутствуют.

Российская Федерация

В Кодексе Российской Федерации об административных правонарушениях содержатся следующие нормы, касающиеся обеспечения безопасности критической информационной инфраструктуры.

Статья 13.12.1 «Нарушение требований в области обеспечения безопасности критической информационной инфраструктуры Российской Федерации»

1. Нарушение требований к созданию систем безопасности значимых объектов критической информационной инфраструктуры Российской Федерации и обеспечению их функционирования либо требований по обеспечению безопасности значимых объектов критической информационной инфраструктуры Российской Федерации, установленных федеральными законами и принятыми в соответствии с ними иными нормативными правовыми актами Российской Федерации, если такие действия (бездействие) не содержат признаков уголовно наказуемого деяния.

2. Нарушение порядка информирования о компьютерных инцидентах, реагирования на них, принятия мер по ликвидации последствий компьютерных атак, проведенных в отношении значимых объектов критической информационной инфраструктуры Российской Федерации, установленного федеральными законами и принятыми в соответствии с ними иными нормативными правовыми актами Российской Федерации.

3. Нарушение порядка обмена информацией о компьютерных инцидентах между субъектами критической информационной инфраструктуры Российской Федерации, между субъектами критической информационной инфраструктуры Российской Федерации и уполномоченными органами иностранных государств, международными, международными неправительственными и иностранными организациями, осуществляющими деятельность в области реагирования на компьютерные инциденты.

Статья 19.7.15 «Непредставление сведений, предусмотренных законодательством в области обеспечения безопасности критической информационной инфраструктуры Российской Федерации»

1. Непредставление или нарушение сроков представления в федеральный орган исполнительной власти, уполномоченный в области обеспечения безопасности критической информационной инфраструктуры Российской Федерации, сведений о результатах присвоения объекту критической информационной инфраструктуры Российской Федерации одной из категорий значимости, предусмотренных законодательством в области обеспечения безопасности критической информационной инфраструктуры Российской Федерации, либо об отсутствии необходимости присвоения ему одной из таких категорий либо представление недостоверных сведений.

Повторное совершение данного правонарушения влечет за собой привлечение к ответственности с увеличенной по размеру санкцией.

2. Непредставление или нарушение порядка либо сроков представления в государственную систему обнаружения, предупреждения и ликвидации последствий компьютерных атак на информационные ресурсы Российской Федерации информации, предусмотренной законодательством в области обеспечения безопасности критической информационной инфраструктуры Российской Федерации.

Республика Таджикистан

Административно-деликтные нормы, касающиеся обеспечения безопасности критической информационной инфраструктуры, в Кодексе Республики Таджикистан об административных правонарушениях отсутствуют.

Вышеприведенные правоположения показывают, что административно-деликтная защита отношений в области обеспечения безопасности критической информационной инфраструктуры из всех государств – членов ОДКБ осуществляется только в Республике Казахстан и Российской Федерации.

Общий вывод и рекомендации

В настоящее время уголовно-правовая защита отношений в области обеспечения безопасности критической информационной инфраструктуры осуществляется только в трех из шести государств – членов ОДКБ – Республике Казахстан, Кыргызской Республике и Российской Федерации. Административно-деликтная защита данных отношений установлена только в Республике Казахстан и Российской Федерации.

С учетом важности обеспечения безопасности критической информационной инфраструктуры для государственной и военной безопасности всех государств – членов ОДКБ целесообразно предложить Республике Армения, Республике Беларусь и Республике Таджикистан

рассмотреть вопрос о введении в их уголовное законодательство специализированных уголовно-правовых норм, направленных на обеспечение правовой защиты данных отношений.

Поскольку наряду с уголовно-правовой защитой эффективным следует признать осуществление правовой защиты отношений в области обеспечения безопасности критической информационной инфраструктуры посредством установления административных наказаний, также целесообразно предложить Республике Армения, Республике Беларусь, Кыргызской Республике и Республике Таджикистан рассмотреть вопрос об установлении административной ответственности за правонарушения в области обеспечения безопасности критической информационной инфраструктуры, обеспечив системную связь такой ответственности в необходимом объеме с уголовным законодательством данных государств.

Важным также представляется установление единообразия подходов к формулированию соответствующих составов преступлений и правонарушений, связанных с безопасностью критической информационной инфраструктуры, во всех государствах – членах ОДКБ.