Анатолий М. Тарасов
Академия управления МВД России,
ул. Зои и Александра Космодемьянских, 8, г. Москва, 125993, Россия
e-mail: Tarasov.tam@yandex.ru, https://orcid.org/0000-0003-0000-408X

СТРУКТУРА И СОДЕРЖАНИЕ КОНВЕНЦИИ ПО ПРОТИВОДЕЙСТВИЮ КИБЕРПРЕСТУПЛЕНИЯМ

DOI: http://dx.doi.org/10.26583/bit.2018.4.05

Аннотация. В статье актуализируется проблема противодействия киберпреступлениям на основе консолидации международных усилий в данном направлении наряду с противодействиями терроризму, обороту наркотиков и другими правонарушениями, имеющими трансграничный характер. Приводятся результаты критического анализа структуры и содержания основных положений соответствующей Будапештской конвенции, принятой Советом Европы 23 ноября 2001г. (ETS № 185). Анализ отражения в Конвенции вопросов организационно-правового регулирования борьбы с компьютерной преступностью проведен в сравнении с соответствующими нормами российского законодательства, в частности по терминологическим аспектам уголовного и уголовно-процессуального права в области компьютерной информации. Особое внимание обращается на критическое рассмотрение вопросов международного сотрудничества в свете новых вызовов и угроз в условиях все возрастающей конфронтации межгосударственных отношений. В заключение обосновывается необходимость принятия соответствующей конвенции Организацией Объединенных Наций с предложениями по содержанию ее основных направлений.
Ключевые слова: Конвенция Совета Европы, правоохранительные и судебные органы, правоохранительная деятельность, киберпреступность, международное сотрудничество, конфиденциальность, компьютерная техника, расследование, программное обеспечение, пароли и коды доступа, детская порнография, авторское право.
Для цитирования: ТАРАСОВ, Анатолий М. СТРУКТУРА И СОДЕРЖАНИЕ КОНВЕНЦИИ ПО ПРОТИВОДЕЙСТВИЮ КИБЕРПРЕСТУПЛЕНИЯМ. Безопасность информационных технологий, [S.l.], v. 25, n. 4, p. 52-62, 2018. ISSN 2074-7136. Доступно на: <https://bit.mephi.ru/index.php/bit/article/view/1167>. Дата доступа: 19 nov. 2018. doi:http://dx.doi.org/10.26583/bit.2018.4.05.

Anatoly M. Tarasov
Management Academy of the Ministry of the Interior of Russia,
Zoi and Alexandra Kosmodemianskikh str., 8, Moscow, 125993, Russia
e-mail: Tarasov.tam@yandex.ru, https://orcid.org/0000-0003-0000-408X

The structure and content of the convention on combating cybercrime

DOI: http://dx.doi.org/10.26583/bit.2018.4.05

Abstract. Consolidation of international efforts plays a crucial role in combating cybercrime the same way as in counteracting to terrorism, drug trafficking and other offenses of cross-border nature. The results of a critical analysis of the structure and content of the major provisions of the Budapest European Convention of 23 November 2001 (ETS No. 185) are presented. The paper provides a comparative analysis of the Convention and the Russian legislation from the point of view of organizational and legal regulation of fight against computer crime. The accent is made on terminological aspects of criminal and criminal procedure law in the field of computer information. Particular attention is drawn to the critical consideration of issues of international cooperation in the light of new challenges and threats of an increasingly confrontational inter-state relations. The conclusion substantiates the need for the adoption of the relevant United Nations Convention with proposals on the content of its main statements.
Keywords: Council of Europe Convention, law enforcement and judicial authorities, law enforcement, cybercrime, international cooperation, privacy, computer technology, investigation, software, passwords and access codes, child pornography, copyright.
For citation: TARASOV, Anatoly M. The structure and content of the convention on combating cybercrime. IT Security (Russia), [S.l.], v. 25, n. 4, p. 52-62, 2018. ISSN 2074-7136. Available at: <https://bit.mephi.ru/index.php/bit/article/view/1167>. Date accessed: 19 nov. 2018. doi:http://dx.doi.org/10.26583/bit.2018.4.05.

Введение

Актуальность и важность рассмотрения данной темы связана с тем, что сегодня международное взаимодействие по противодействию киберпреступности ослабевает, все большее количество государств предпринимают шаги для получения господства в информационном пространстве. Во многих странах созданы и активно действуют кибервойска. Милитаризация киберпространства усиливает масштабы проявлений информационных войн, направленных против мира и безопасности. При этом основные угрозы нацелены на подрыв политической, экономической и социальной систем других государств, массированную психологическую обработку населения, сфокусированную на дестабилизации работы государственных и общественных институтов, в том числе с целью проведения так называемых «цветных революций» [1].

Постоянно увеличивается количество кибератак на сайты органов государственной власти других государств, все чаще атакуются критически важные объекты экономической и военной инфраструктуры, бизнеса, особенно банковского сектора [2].

Человечество сегодня столкнулось с серьезными рисками и вызовами, связанными с растущей латентностью киберпреступлений, их организованностью и глобализацией. Среди наиболее распространенных видов киберпреступлений в международном плане можно выделить создание, распространение и использование вредоносных программ, взлом паролей, кражу банковских реквизитов для совершения различных преступлений, распространение противоправной информации (клеветы, порнографических материалов и т.д.). Большую распространенность получили DdoS-атаки и финансовые киберпреступления, нацеленные на похищение платежных данных пользователей интернет-банкинга, платежных карт, а также непосредственно денег со счетов компаний и отдельных пользователей [3]. Одна из первых таких проб пера началась с троянца Ibank, в его развитие были созданы ZeuS и SpyEye, затем эту группу пополнили Carberp и Carbanak. Злоумышленники международной группы Carbanak, в которую входили граждане России, Украины, стран Европы и Китая, были установлены при непосредственном участии специалистов Лаборатории Касперского. По имеющимся данным, в 30 странах мира ими было похищено со счетов порядка 100 банков около 1 миллиарда долларов США. Кстати, о значительном росте киберугроз свидетельствуют следующие данные. Еще четыре-пять лет назад антивирусные ресурсы Лаборатории Касперского обнаруживали в течение суток порядке 125 – 150 тыс. вредоносных объектов, а в настоящее время – порядка 300 тыс. (рост в два раза).

Все более серьезную опасность представляют так называемые «умные дома», «умные квартиры», оборудованные «умными вещами» (телевизорами, стиральными машинами, кофеварками и другими бытовыми приборами, а также автомототранспортом). Такие вещи, подключенные к Интернету, программы которых требуют периодической прошивки, обновления, фиксируют и могут передавать информацию о наших привычках, интересах, с кем общаемся, интимных особенностях, то есть персональные качества. Принцип приватности все больше девальвируется.

Таким образом, можно сделать вывод, что борьба с киберпреступностью и новыми кибервызовами в международном формате наряду с проблемами борьбы с терроризмом, незаконным оборотом наркотиков, оружия, коррупцией является одной из наиболее сложных и требующих особого и постоянного внимания международного сообщества.

Масштабность киберугроз по логике вещей должна нацеливать различные государства на объединение усилий по созданию эффективных международных организационно-правовых механизмов по противодействию киберправонарушениям, однако, к сожалению, особенно в последние годы международные связи в этом направлении ослабли, эффективность противодействия киберпреступности существенно не возрастает. Вместе с тем именно нарастание в 90-е годы киберугроз способствовало принятию Советом Европы 23 ноября 2001 г. в Будапеште Европейской конвенции по

противодействию киберпреступлениям (ETS № 185) [4][1] (далее – Конвенция).

Анализ основных положений Конвенции

Сегодня все большее количество государств видят решение проблемы повышения эффективности противодействия киберпреступности в реализации принципа «неделимости безопасности кибепространства», то есть в применении правила-запрета отдельному государству добиваться господства в информационном пространстве над другими государствами. При этом учитывается, что решение этой проблемы заключается в совершенствовании механизмов сотрудничества, организационного, правового, финансового, кадрового, технического, информационного, научно-методического обеспечения деятельности правоохранительных и судебных органов власти.

На решение многих из указанных выше проблем нацелены положения Конвенции по противодействию киберпреступлениям, необходимость их реализации актуальна и востребована по сей день.

Слово и понятие «киберпреступность» используется в различных значениях, в том числе как компьютерная преступность[2] [5], преступность в сфере компьютерных технологий, компьютерной информации [6]. Эти понятия, как правило, воспринимаются как тождественные.

Под киберпреступлениями, как правило, понимаются преступные деяния, посягающие на информационную безопасность и совершенные в виртуальном пространстве с применением компьютерных технологий. Предметом их являются информация и компьютерные средства. При этом компьютер, его программное обеспечение являются либо орудием, либо предметом, либо средством посягательств.

Анализ положений Конвенции показывает, что их содержательная часть нацелена на создание эффективного организационно-правового механизма сотрудничества между государствами – членами Конвенции, а также организациями и частными лицами. Основной идеей данного документа стало установление единообразного международного подхода к составам компьютерных преступлений, которые государства должны включить в свое национальное законодательство, а также разработка мер по предотвращению правонарушений, направленных против целостности, доступности, конфиденциальности информации, компьютерных систем, сетей, данных, а также неправомерного их использования. Целью принятия Конвенции также является установление путей применения властных полномочий, способствующих обнаружению, расследованию и судебному преследованию за совершение кибердеяний с учетом соблюдения прав человека. Отметим при этом, что для государств, подписавших Конвенцию, большинство её положений несут не обязательный, а рекомендательный характер.

Анализ структуры и содержания показывает, что Конвенция охватывает три основных направления:

- согласование национальных правовых норм, определяющих составы соответствующих преступлений;
- формирование процедуры расследования киберпреступлений;
- создание действенной системы межгосударственного сотрудничества в сфере противодействия киберпреступности.

[1] Текст Конвенции размещен на ресурсе СПС «Гарант»: http://base.garant.ru/4089723/#ixzz5WwK9w8it. Российская Федерация к Конвенции не присоединилась, поскольку Россию, как и ряд других стран, не устраивает установленное в ст. 32 Конвенции право спецслужб одних стран проникать в киберпространство других стран и проводить там операции, не ставя в известность местные власти. За прошедший период к Конвенции присоединились или её подписали порядка 50 стран.

[2] См.: например: А.Я. Минин О специфике противодействия киберпреступности // Российский следователь. 2013. № 8; Чекунов И.Г. Киберпреступность: понятие и классификация // Российский следователь. 2012. №24.

Структура и содержание Конвенции

Рассмотрим подробнее содержание и структуру Конвенции.

В главе 1 Конвенции дается толкование терминов, связанных с содержанием данного международного документа. Например, дефиниция «компьютерная система» означает любое устройство или совокупность соединенных между собой или связанных устройств, одно либо более из которых осуществляет автоматическую обработку данных в соответствии с программой.

При этом отметим, что в российском законодательстве используется такой сходный термин, как «информационная система» [7]. Под ней в соответствии со статьей 2 Федерального закона от 27 июля 2006 г. № 149-ФЗ «Об информации, информационных технологиях и о защите информации» понимается «совокупность содержащейся в базах данных информации и обеспечивающих ее обработку информационных технологий и технических средств».

В Конвенции дается понятие термина «компьютерные данные» – это любое представление фактов, информации или концепций в форме, подходящей для обработки в компьютерной системе, в том числе это программы, предназначенные для выполнения компьютерной системой определенных действий. Следует сказать, что в примечании 1 к статье 272 УК РФ используется термин «компьютерная информация». Под компьютерной информацией понимаются сведения (сообщения, данные), представленные в форме электрических сигналов, независимо от средств их хранения, обработки и передачи.

В свою очередь под «данными трафика» (передвижения) в Конвенции понимаются любые компьютерные данные, связанные с операциями по их передаче посредством компьютерной системы, которые созданы компьютерной системой, являющейся звеном в цепочке передачи данных, и указывают на источник сообщения, его назначение, маршрут, время, дату, размер, длительность или тип лежащей в его основе услуги. Кроме того, в Конвенции дается определение «сервис-провайдера» или «поставщика услуг» – это любая государственная или частная организация (юридическое лицо), предоставляющая своим пользователям возможность обмениваться данными (коммуникационные услуги) посредством компьютерной системы, а также любая иная организация, которая обрабатывает или хранит компьютерные данные по поручению организации, предоставляющей коммуникационные услуги, либо пользователей таких услуг.

В разделе 2 главы 1 Конвенции перечисляются меры в области материального уголовного права, которые следует принять государствам в целях реализации положений Конвенции на национальном уровне.

Согласно Конвенции, к объектам киберпреступлений относятся охраняемые нормами права общественные отношения, связанные с информационно-коммуникационными процессами по поводу поиска, сбора, обработки, производства, накопления, хранения, передачи, распространения, потребления компьютерной информации. Для совершения киберпреступления в технико-технологическом плане необходимо наличие компьютерного устройства, компьютерных систем, соответствующего программного обеспечения, сети.

Анализ положений второй главы показывает, что структура киберпреступлений в Конвенции представлена четырьмя группами общественно опасных деяний.

В части 1 главы 2 Конвенции рассматриваются преступления против конфиденциальности, целостности и доступности компьютерных данных и систем. В частности, **в статье 2 названо такое правонарушение, как «незаконный доступ», в статье 3 «незаконный перехват», в статье 4 «вмешательство в данные», в статье 5 «вмешательство в систему, в статье 6 «ненадлежащее использование устройств».**

В части 2 главы 2 Конвенции рассматриваются преступления, связанные с компьютерами, такие как: **«подлог компьютерных данных» (ст. 7), «компьютерное мошенничество» (ст. 8). Статья 9 части 3** посвящена деяниям, связанным с содержанием контента, в частности **с детской порнографией. В статье 10 части 4** Конвенции рассматриваются преступления, связанные с нарушениями авторского права и смежных прав.

Статья 11 части 5 главы 2 посвящена вопросам, связанным с дополнительной ответственностью и санкциями, в частности, в связи **с покушением, пособничеством и подстрекательством в совершении киберпреступления. Кроме того, в статье 12 части 5 рассматриваются вопросы коллективной ответственности. Следует отметить, что статья 13 части 5 посвящена санкциям и мерам за совершение киберпреступлений. В ней акцент делается на то, что стороны Конвенции** должны принять меры законодательного и иного характера, которые бы гарантировали, что лица, совершившие киберпреступления, будут наказаны действенными, соразмерными и убедительными санкциями, включающими в себя лишение свободы.

Таким образом, в Конвенции установлен перечень мер, которые должны принимать страны в отношении совершенных кибердеяний против конфиденциальности, целостности и доступности компьютерных данных и систем; правонарушений, связанных с компьютерами; правонарушений, относящихся к детской порнографии, а также связанных с нарушением авторских и смежных прав.

В Конвенции также установлено, что состав уголовно наказуемого правонарушения определяется наличием следующих условий:

а) совершенное деяние должно повлечь за собой ответственность;

б) при этом деяние должно быть совершено умышленно и противоправно.

Таким образом, для установления наличия состава преступления необходимо, чтобы в уголовном законодательстве соответствующего государства было предусмотрена ответственность за такое деяние, только тогда деяние становится противоправным, а также необходимо, чтобы преступление было совершено умышленно. Итак, в Конвенции определено, что преступной является деятельность, если её осуществление не санкционировано государством в установленном законном порядке.

Кстати, в российском уголовном законодательстве данное положение Конвенции нашло прямое отражение, в том числе в главе 28 УК РФ, именуемой «Преступления в сфере компьютерной информации», и других нормах. Так, в статье 272 УК РФ уголовное наказание предусмотрено за неправомерный доступ к охраняемой законом компьютерной информации, в статье 273 – за создание, распространение или использование компьютерных программ либо иной компьютерной информации, заведомо предназначенных для несанкционированного уничтожения, блокирования, модификации, копирования компьютерной информации или нейтрализации средств защиты компьютерной информации, в статье 274 – за нарушение правил эксплуатации средств хранения, обработки или передачи охраняемой компьютерной информации …».

Анализ содержания второй главы Конвенции позволяет сделать вывод о том, что компьютеры, компьютерные сети, программное обеспечение, человеческий ресурс могут быть использованы как в декларированном законом порядке, так и для достижения криминальных целей. В этой связи компьютерные программы в зависимости от субъективных целей фактически могут иметь двойное назначение: позитивное и криминальное – зависит от наличия или отсутствия соответствующего умысла, то есть от субъективного фактора.

Поэтому положения Конвенции, имеющие рекомендательный и дифференцированный характер, считаем вполне оправданными. При внесении изменений в национальные законодательства государства могут руководствоваться национальными факторами (особенностями). Причем Конвенция нацеливает государства на то, что в действиях лица, использующего технические возможности компьютера, его программное обеспечение, а также сети связи, необходимо устанавливать не только наличие или отсутствие преступного замысла, но и достижение его реализации. Ведь цель может быть не достигнута, например, по причинам отказа от доведения криминальной цели до результата в связи с отказом злоумышленника, либо по причине того, что не сработало программно-техническое обеспечение (покушение на преступление).

Отметим при этом, что компьютерные программы, состоящие из различных элементов, а также каждый элемент по отдельности могут быть задекларированы, но тем не

менее программа может быть использована для совершения, например, неправомерного удаленного доступа к охраняемой законом компьютерной информации. Или наоборот, некоторые включенные в программу элементы, их функции могут быть не задекларированы и использованы для достижения преступных целей, однако программа в целом, считается, не предоставляет таких технологических возможностей. Подход в таких случаях должен быть дифференцированным, и в законодательствах должны быть учтены и такие обстоятельства.

В этой связи в статье 273 УК РФ речь, очевидно, должна идти и об уголовной ответственности за создание отдельных элементов, которые могут быть использованы либо используются для создания программ, позволяющих применять их в преступных целях, причем как создателями, так и другими лицами. То есть важно учитывать, что одни лица создают элементы (составные части) или целые криминальные программы, другие их перепродают, не всегда зная об их криминальных ресурсах, а третьи их применяют в различных целях.

Понятно, что установить злоумышленников, обнаружить недекларируемые технологические элементы и их следы в программно-техническом обеспечении компьютера непросто[8], а доказать их преступную направленность, тем более до совершения криминального деяния, вообще крайне сложно. Нужны высокопрофессиональные специалисты и передовые технологии. Их отсутствие напрямую способствует высокой латентности совершенных киберпреступлений.

В этой связи и в целях повышения эффективности деятельности по профилактике киберпреступлений в уголовном законодательстве важно предусматривать различные аспекты, в том числе цели, признаки, стадии производства и использования программно-технического потенциала.

Перейдем к рассмотрению второго раздела второй главы Конвенции, именуемого «Процессуальные нормы». В нем установлены нормы, определяющие процедуру расследования компьютерных преступлений, то есть процессуальные вопросы борьбы с киберпреступностью. В частности, прописаны следующие аспекты, связанные с киберпреступностью:

– защита хранящихся в компьютерах данных;

– обеспечение безопасности хранения и оперативного представления данных о трафике;

– поиск и арест электронных систем;

– фиксация трафика, перехват сетевого контента.

При этом отметим, что статья 14 Конвенции содержит положение, относящееся к государствам – членам Конвенции, о необходимости нормативного правового обеспечения использования компьютерных систем и сбора доказательств в электронной форме при расследовании киберпреступлений, а статья 19 предусматривает расширение полномочий правоохранительных органов в первую очередь в части правовой регламентации их деятельности, касающихся осуществления оперативно-розыскных мероприятий в отношении компьютерных систем и носителей компьютерных данных. В этом связи можно сделать вывод о том, что Конвенция не просто рекомендует, а и обязывает государства – члены Конвенции создавать правовые возможности для ведения активного противодействия киберпреступности, включая наделение, например, субъектов оперативно-розыскной деятельности правом:

– выемки компьютерной системы, ее частей или носителей;

– конфискации копий компьютерных данных;

– уничтожения или блокировки компьютерных данных, находящихся в компьютерной системе;

– обеспечения целостности и сохранности хранящихся компьютерных данных,

относящихся к конкретному делу[3].

При этом следует отметить, что основные задачи оперативно-розыскной деятельности (ОРД) согласно статье 2 Закона об ОРД состоят в выявлении, предупреждении, пресечении и раскрытии преступлений, а также в установлении лиц, их подготавливающих, совершающих или совершивших, скрывающихся от органов дознания, следствия и суда. Перечень допустимых оперативно-розыскных мероприятий указан в статье 6 этого Закона. К ним, в частности, относятся: исследование предметов, … снятие информации с технических каналов связи[4] [9].

При решении задач ОРД субъекты оперативно-розыскной деятельности правоохранительных органов имеют право (статья 15 Закона об ОРД) производить изъятие документов, предметов, материалов и сообщений, прерывать предоставление услуг связи в случае возникновения непосредственной угрозы жизни и здоровью лица, а также угрозы государственной, военной, экономической, информационной или экологической безопасности Российской Федерации. Поясним, что при копировании документов и (или) информации, содержащейся на изымаемых электронных носителях информации, должны обеспечиваться условия, исключающие возможность утраты или изменения документов и (или) информации.

В соответствии с требованиями статьи 8 Закона Об ОРД проведение оперативно-розыскных мероприятий, которые ограничивают конституционные права человека и гражданина на тайну переписки, телефонных переговоров, сообщений, передаваемых по сетям электрической связи, допускается на основании судебного решения и при наличии у субъектов ОРД установленной в Законе соответствующей информации.

Вместе с тем нужно сказать, что нормы Конвенции, касающиеся процессуальных решений и действий, как показывает их анализ, не обеспечивают в полном объеме унификацию процедуры раскрытия и расследования компьютерных преступлений, а также судебного преследования за их совершение, по которым сбор доказательств проводится с применением электронных средств и способов. Конвенция в этой части, на наш взгляд, регулирует только содержание отдельных розыскных, следственных и судебных действий.

При этом целый ряд достаточно важных процессуальных вопросов оставлен на усмотрение государств (сторон), её подписавших. Например, какие органы могут быть наделены полномочиями давать указания о сохранности электронных данных, об их предъявлении, блокировке и т. п. И такой подход является оправданным, поскольку на практике возникают проблемы, связанные с наличием/отсутствием соответствующей компетенции у тех или иных правоохранительных и судебных органов конкретного государства. Кстати, в различных государствах такими полномочиями наделены либо следственные, либо судебные органы, либо те и другие. В этой связи различается по своей процедуре и проведение процессуальных мероприятий.

Отметим также, что в Конвенции установлено, что государства-участники должны принять такие законодательные и иные меры, какие будут необходимы, чтобы обязать определенную структуру, лицо хранить компьютерные данные и обеспечивать их сохранность в течение адекватного периода времени. В этой связи возникает вопрос о длительности «адекватного» периода времени, а также о том, какие субъекты будут это устанавливать (государство в своём законодательстве или уполномоченные государственные органы в каждом конкретном случае).

Важное значение в Конвенции для ее ратификации имеет статья 20 «Сбор данных трафика в режиме реального времени» и статья 21 «Перехват данных содержания». В них установлены нормы, определяющие необходимость формирования национальной

[3] В России подобными правами в соответствии со ст. 13 Федерального закона от 12 августа 1995 г. «Об оперативно-розыскной деятельности» наделены, например, специальные подразделения МВД России, ФСБ России), ФСО России, СВР России, ФСИН России, ФТС России, Главного управления (ГРУ) Минобороны России.

[4] Н.В. Павличенко Правовые и теоретические проблемы обеспечения негласности в оперативно-розыскной деятельности. Монография. М: 2016. 185 с.

нормативной базы, обязывающей сервис-провайдеров проводить сбор, фиксацию, перехват необходимой информации с помощью имеющихся у них технических средств. Причем речь идет о сборе компьютерных данных в режиме реального времени. В решении таких вопросов сервис-провайдеры обязываются при сохранении полной конфиденциальности о фактах сотрудничества с правоохранительными органами способствовать их деятельности.

Принятый в России так называемый «Закон Яровой» (Федеральный закон от 6 июля 2016 года № 374-ФЗ, вносящий изменения в п.1 ст. 64 Федерального закона "О связи") предписывает операторам связи и организаторам распространения информации в сети «Интернет» хранить записи звонков и переписку своих абонентов и пользователей до шести месяцев, а информацию о фактах коммуникаций – до трех лет.

Раздел III Конвенции именуется «Международное сотрудничество».

Этот раздел посвящен в основном вопросам экстрадиции и совместной деятельности государств – участников Конвенции по противодействию киберпреступлениям, достижения согласованности при сборе доказательств в электронной форме. Кроме того, в разделе определены общие для всех интернет-провайдеров международные правила хранения личной информации клиентов на случай, если такая или подобная информация будет затребована, например, правоохранительными органами в ходе расследования киберпреступлений.

Вопросы, связанные с экстрадицией, нашли непосредственное отражение в статье 24 Конвенции, где указывается, что экстрадиция применима, если совершены преступления, установленные в статьях 2 – 11 Конвенции и, если за эти преступления в законодательствах государств предусмотрена ответственность в виде лишения свободы на один год или более строгая мера ответственности. Важно отметить, что для государств, между которыми отсутствуют соглашения о выдаче преступников, но они являются сторонами Конвенции, данная норма является юридическим основанием для экстрадиции лиц, совершивших преступления, указанные в статьях 2 – 11 Конвенции.

В статье 25 Конвенции сформулированы общие принципы взаимной помощи государств – участников Конвенции, в статье 26 – порядок добровольного предоставления информации, в статье 27 определены принципы направления и выполнения запросов о содействии в случае отсутствия соответствующих международных соглашений, в статье 28 – принципы конфиденциальности и ограниченного использования информации. Перечисленные статьи (принципы) Конвенции нацелены в том числе на защиту прав и свобод человека и гражданина. Так, в статье 28 установлено, что государства обязаны соблюдать требования о конфиденциальности запросов об экстрадиции и не использовать полученную информацию в целях, не указанных в запросе. Адреса организаций соответствующего государства – стороны Конвенции, ответственной за подготовку запросов об экстрадиции или организации арестов, вносятся в регистр Генерального секретаря Совета Европы.

Помимо традиционных форм международного сотрудничества, регулируемого такими документами, как Европейская конвенция о выдаче (экстрадиции) от 13.12.1957 г. (ETS № 24)[5] и Европейская конвенция о взаимной правовой помощи по уголовным делам[6], принятой в Страсбурге 20 апреля 1959 г., в Конвенции по противодействию киберпреступлениям предусматривается осуществление международного сотрудничества, благодаря которому правоохранительные органы одних государств могут собирать хранимую на электронных носителях (компьютерах) информацию и улики, не проводя при этом трансграничных расследований и розыска [10].

К формам оказания правовой помощи по уголовным делам относится и установленная в Конвенции возможность применения электронных и факсимильных средств и способов связи, включая шифрование, в виртуальном пространстве, в частности, при направлении

[5] Собрание законодательства РФ. 25.10.1999. № 43. Ст. 5129. Конвенция ратифицирована.
[6] Собрание законодательства РФ. 05.06.2000. № 23. Ст. 2349. Конвенция ратифицирована с оговорками Федеральным законом от 25.10.1999 г. № 193-ФЗ.

запросов и получении на них ответов (ст. 25 Конвенции).

Как показывает анализ содержания Конвенции, принципиальное значение для её подписания имеет статья 32, именуемая «Трансграничный доступ к компьютерным данным, находящимся в системах общего доступа, либо при получении соответствующего разрешения». В пункте b) статьи 32 установлено право любой из сторон без согласия другой стороны посредством компьютерной системы на своей территории получать трансграничный доступ к данным, которыми располагает другая сторона, без уведомления властей данного государства, располагающего соответствующей информацией, и в первую очередь это касается персональных (личных) данных. Такой правовой механизм позволяет нарушать фундаментальные гражданские права человека и гражданина. Получается, что каждое государство, подписавшее Конвенцию, с помощью действующих на его территории провайдеров может контролировать информационный обмен в Сети. Как известно, основные провайдеры и их электронные ресурсы находятся на территории США, и у этой страны на этот счет имеются огромные преимущества. В то же время многие государства – стороны Конвенции не имеют такой технологической возможности, и данная норма для них является в основном декларативной, но обязательной для исполнения.

Кстати, отметим, что одним из противоречивых мест Конвенции является то, что, с одной стороны, в ней в качестве преступных деяний конкретно не указываются различные посягательства на конфиденциальность личных данных, с другой, согласно статье 10 Конвенции «О защите физических лиц в отношении автоматизированной обработки данных личного характера», государства – стороны Конвенции обязываются ввести в свое законодательство санкции за нарушение конфиденциальности личных данных.

Подчеркнем, что относиться к содержанию статьи 32 Конвенции можно по-разному. Положительная её направленность, в частности, проявляется в том, что эта норма позволяет получать трансграничный доступ к информации без бюрократических запросов, например, в ситуации, когда преступник и жертва находятся на территориях различных стран и в различной юрисдикции. Вместе с тем данной нормой создан общий механизм, позволяющий бесконтрольно правоохранительным органам одного государства непосредственно действовать в сфере юрисдикции другого государства, не прибегая к получению разрешения этого государства.

В этой связи отметим, что в основном именно из-за этой нормы целый ряд государств, в том числе Россия, не принимают решения о присоединении к Конвенции. Кстати, сам механизм присоединения к Конвенции определен в статьях 36 и 37. Так, в статье 36 установлено, что Конвенция открыта для подписания государствами – членами Совета Европы и государствами, не являющимися его членами, но участвовавшими в ее разработке, как, например, Россия.

Согласно статье 37 к Конвенции может присоединиться любое государство и вне Европы, но для этого необходимо согласие большинства государств – участников Конвенции. В этой гибкой процедуре проявляется значительный международный потенциал присоединения к Конвенции. Такой порядок, считаем, обоснован тем, что мировое сообщество крайне обеспокоено растущей опасностью, исходящей от киберугроз и стремится обеспечить международную безопасность киберпространства на основе глобального сотрудничества.

Заключение

В заключение отметим, что несмотря на некоторую противоречивость, Конвенция на сегодняшний день является одним из основных международных актов для развития национальных законодательств по противодействию киберпреступности, создания механизма государственного контроля за обращением компьютерных данных в связи с совершением киберправонарушений. Указанные в Конвенции разнообразные процессуальные действия позволяют сохранять, собирать, перехватывать и изымать информацию, являющуюся объектом и/или средством преступного посягательства.

При этом подчеркнем, что современные тенденции масштабного и трансграничного распространения киберпреступности, активно расширяющийся её глобальный характер обуславливают необходимость дальнейшего развития международного сотрудничества по противодействию киберугрозам в более широком формате – в рамках Организации Объединенных Наций (ООН). В этой связи на сегодняшний день важной задачей является принятие Конвенции ООН по кибербезопасности.

В проект данной Конвенции представляется необходимым включить следующие обязывающие государства принципы:

– невмешательства в информационное пространство друг друга, то есть неиспользования IT-технологий для вмешательства в дела, относящиеся к внутренней компетенции другого государства;

– неделимости обеспечения безопасности кибепространства;

– несовершения шагов, которые могли бы привести к усилению киберугроз;

– невмешательства во внутренние дела других государств, в частности для организации так называемых «цветных революций»;

– невключения в национальные нормативные правовые акты норм реагирования на кибератаки посредством применения ядерного оружия;

– неограничения доступа граждан в информационное пространство, за исключением случаев обеспечения национальной безопасности;

– сотрудничества при расследовании трансграничных кибератак (киберпреступлений).

СПИСОК ЛИТЕРАТУРЫ:

1. Макаренко С.И. Информационное противоборство и радиоэлектронная борьба в сетецентрических войнах начала XXI века. Монография. — СПб.: Наукоемкие технологии, 2017. — 546 с. (URL - http://publishing.intelgr.com/archive/Makarenko-InfPro.pdf. (Дата доступа 14.10.2018).
2. Угрозы информационной безопасности в кризисах и конфликтах XXI века/Под редакцией А.В. Загорского, Н.П. Ромашкиной. – М: ИМЭМО РАН, 2015. – 151 с. (URL - https://www.imemo.ru/files/File/ru/publ/2015/2015_027.pdf, дата доступа 14.10.2018).
3. Казарин О.В., Скиба В.Ю., Шаряпов Р.А. Новые разновидности угроз международной информационной безопасности. Вестник РГГУ. Серия: Документоведение и архивоведение. Информатика. Защита информации и информационная безопасность. 2016. № 1 (3). С. 54 – 72.
4. Конвенция о преступности в сфере компьютерной информации ETS № 185 (Будапешт, 23 ноября 2001) URL: http://base.garant.ru/4089723/#ixzz5WwK9w8it (Дата доступа: 10.10.2018).
5. Минин А. Я. О специфике противодействия киберпреступности // Российский следователь. 2013. № 8. С. 37 – 39.
6. Чекунов И. Г. Киберпреступность: понятие, классификация, современные вызовы и угрозы // Молодые ученые. Издательство: Московский институт государственного управления и права (Москва). 2012. № 3. С. 178 – 186. URL: https://elibrary.ru/item.asp?id=21944441 (Дата доступа: 10.10.2018).
7. Тарасов А.М. Электронное правительство и информационная безопасность. Учебное пособие. М: Галарт, 2011. – 648 с.
8. Durakovsky, A. P., Melnikov, D. A., Gorbatov, V. S., Ivanenko, V. G. and Modestov, A. A., "Russian Model of Public Keys and Validation Infrastructure as Base of the Cloud Trust," 2016 IEEE 4th International Conference on Future Internet of Things and Cloud (FiCloud)(FICLOUD), Vienna, Austria, 2016, pp. 123 – 130. doi:10.1109/FiCloud.2016.
9. Павличенко Н.В. Правовые и теоретические проблемы обеспечения негласности в оперативно-розыскной деятельности. Монография. М: 2016. – 185 с.
10. Hannigan R. The web is a terrorist's command-and-control network of choice // The Financial Times [Электронный ресурс]. URL: http://www.ft.com/cms/s/2/c89b6c58-6342-11e4-8a63-00144feabdc0.html#axzz3I2F0l6FM (Дата доступа: 17.10.2018).

REFERENCES:

[1] Makarenko S.I. Information warfare and electronic warfare in the network-centric wars of the early XXI century. Monograph. — SPb.: Naukoemrie texnologii, 2017. — 546p. (URL - http://publishing.intelgr.com/archive/Makarenko-InfPro.pdf (Access date: 14.10.2018)]. (in Russian).
[2] Informational Security Threats in Crises and Conflicts of XXI Century/ a.v. Zagorskii, N.P. Romashkina, eds. – Moscow, 2015. – 151p. (in Russian).

[3] Kazarin, O.V., eds. New types of threats to international information security. Vestnik RGGU. Seriya: Dokumentovedenie i arhivovedenie. Informatika. Zashchita informacii i informacionnaya bezopasnost'. 2016. № 1 (3). p. 54 – 72. (in Russian).
[4] Convention on crime in the sphere of computer information ETS N 185 (Budapest, November 23, 2001) URL: http://base.garant.ru/4089723/#ixzz5WwK9w8it (Access date: 10.10.2018).
[5] Minin, A.Ya. On the specifics of combating cybercrime. Rossijskij sledovatel'. 2013. №8. p. 37 – 39. (in Russian).
[6] Chekunov, I. G. Cybercrime: concept, classification, modern challenges and threats. Molodye uchenye. Publisher: Moscow Institute of public administration and law (Moscow). 2012. № 3. С. 178 – 186. URL: https://elibrary.ru/item.asp?id=21944441 (Access date: 10.10.2018) (in Russian).
[7] Tarasov, A.M. E - government and information security. Textbook. M: Galart, 2011. – 648 p. (in Russian).
[8] Durakovsky, A.P., Melnikov, D.A., Gorbatov, V.S., Ivanenko, V.G. and Modestov, A.A., "Russian Model of Public Keys and Validation Infrastructure as Base of the Cloud Trust," 2016 IEEE 4th International Conference on Future Internet of Things and Cloud (FiCloud)(FICLOUD), Vienna, Austria, 2016, pp. 123 - 130. doi:10.1109/FiCloud.2016.
[9] Pavlichenko, N.V. Legal and theoretical problems of ensuring secrecy in operational-search activity. Monograph. M: 2016. – 185 p. (in Russian).
[10] Hannigan R. The web is a terrorist's command-and-control network of choice // The Financial Times [Электронный ресурс]. URL: http://www.ft.com/cms/s/2/c89b6c58-6342-11e4-8a63-00144feabdc0.html#axzz3I2F0l6FM (Access date: 17.10.2018).

Поступила в редакцию – 14 октября 2018 г. Окончательный вариант – 15 ноября2018 г.
Received – October 14, 2018. The final version – November 15, 2018.