

МЕЖДУНАРОДНЫЕ СОГЛАШЕНИЯ В СФЕРЕ ПРОТИВОДЕЙСТВИЯ КИБЕРПРЕСТУПНОСТИ: СОВРЕМЕННОЕ СОСТОЯНИЕ

М. Г. Головенчик

*Белорусский государственный университет, г. Минск;
marina.golovenchik@inbox.ru;*

науч. рук. – О. М. Старовойтов, канд. юрид. наук, доцент

В работе акцентируется внимание на киберугрозах, как актуальной разновидности современной преступной деятельности. Отмечается характер и степень общественной опасности таких угроз, анализируются современные международные соглашения, направленные на противодействие международной киберпреступности, ее предупреждение и профилактику. Предпринята попытка классификации данных соглашений, проведен анализ основных положений соглашений, определяющих их нормативное содержание. Были выявлены основные признаки, по которым указанные соглашения разграничиваются между собой, показано соотношение материальной и процессуальной составляющей в нормативном содержании их норм. Установлено, что данные соглашений в настоящее время утрачивают свою актуальность ввиду стремительного развития технического прогресса, появления новых информационно-коммуникационных средств и систем связи.

Ключевые слова: киберпреступность, международная преступность, информационная безопасности, борьба с киберпреступлениями, международное сотрудничество государств

Современные киберугрозы представляют собой одно из наиболее значимых проявлений преступной деятельности, осуществляемой в сфере информационного и телекоммуникационного пространства, выступающего на сегодняшний день безусловным компонентом существования нашего общества. В ходе таких противоправных деяний под угрозу могут быть поставлены различные объекты правовой охраны, обладателями которых могут выступать не только граждане, но и коллективные образования, юридические лица, государство в лице его органов. Результатом преступной деятельности хакеров может явиться саботирование работы ключевых предприятий, обеспечивающих функционирование электросетей, систем водо- и газоснабжения, учреждений здравоохранения, банковской сферы и т.д. История подтверждает факты успешных киберпосягательств на военные объекты, включая Пентагон [1].

Безусловно, подобные противоправные деяния не могут оставаться незамеченными, в связи с чем правоохранительные органы абсолютного большинства государств предпринимают попытки объединить свои усилия с тем, чтобы, действуя совместно, противостоять этому негативному явлению. С этой целью проводятся многочисленные конференции, на которых обсуждаются актуальные вопросы совместного противодейст-

вия киберпреступности, высказываются предложения, направленные на унификацию внутреннего законодательства, разрабатываются проекты международных соглашений в этой сфере.

В последние два десятилетия принято большинство из существующих международных договоров в рассматриваемой области. Как правило, такие договоры носят многосторонний региональный характер, но уже сегодня высказываются предложения о необходимости разработки конвенционного соглашения, которое было бы подготовлено под эгидой Организации Объединенных Наций и носило бы глобальный характер.

Проведенный анализ международных договоров в сфере противодействия киберпреступности позволил выделить пять основных групп таких нормативных актов:

- правовые акты, принятые под эгидой Организации Объединенных Наций (общего характера, направленные на противодействие преступности в целом);
- нормативные акты, разработанные и внедренные в рамках Совета Европы;
- нормативные акты, принятые на территории Содружества Независимых государств либо Шанхайской организации сотрудничества;
- конвенционные и межправительственные африканские соглашения в области борьбы с киберпреступлениями;
- правовые акты, действующие в рамках Лиги арабских государств.

В то же время нужно сказать, что по своему содержанию нормы указанных международных договоров зачастую перекликаются. В них нередко используется одна и та же терминология, в то время как основным критерием разграничения выступают процедурные вопросы, касающиеся взаимодействия государств-участников соглашений и их правоохранительных органов.

Вместе с тем, существует ряд принципиальных различий, первым из которых следует назвать различную юридическую силу заключенных конвенционных соглашений. Так, одни соглашения можно назвать договорами базового уровня, включив в их число, например, Конвенцию Совета Европы о преступности в сфере компьютерной информации, Соглашение о сотрудничестве государств-участников СНГ в борьбе с преступлениями в сфере информационных технологий, Соглашение Шанхайской организации сотрудничества по вопросам обеспечения информационной безопасности, Конвенцию Лиги арабских государств о борьбе с преступлениями в области информационных технологий и др. Такие договоры содержат положения, обязательные для государств-участников. В то же время существуют и такие соглашения, которые облада-

ют лишь рекомендательным характером. К ним относятся, как правило, различные Типовые законы, разработанные в том или ином регионе.

Следующим критерием разграничения необходимо назвать различную географическую протяженность действия соглашений. В тех случаях, когда речь идет о международно-правовых соглашениях, возлагающих на государства-участников определенные обязательства, их территориальная распространенность, как правило, совпадает с границами деятельности той международной организации, под эгидой которой данный нормативный акт был разработан и внедрен. В частности, отдельные нормы, ограничивающие границы действия нормативных положений, можно обнаружить в Преамбуле Конвенции Совета Европы о преступности в сфере компьютерной информации, Преамбуле Соглашения государств-членов СНГ и проч. В то же время известны случаи, когда не все государства, входящие в то или иное экстерриториальное межгосударственное образование, ратифицируют принятое соглашение. С другой стороны, есть и обратные примеры, подразумевающие, что в разработанном международном соглашении могут принимать участие в том числе и иные государства, не входящие в это межгосударственное образование.

Следующим и, пожалуй, основным критерием разграничения международных договоров в рассматриваемой сфере необходимо назвать их содержательно-нормативную составляющую. При этом проведенный анализ показал два основных направления конструирования норм международных соглашений: первое превалирует к закреплению деяний, которые следует признавать преступными (Конвенция Совета Европы о киберпреступлениях, Соглашение, заключенное в рамках Содружества Независимых Государств, и др.); второе – имеет в приоритете закрепление институциональных (процедурных) вопросов, регламентирующих непосредственное взаимодействие государств в противодействии транснациональной киберпреступности (Соглашение, заключенное в рамках Шанхайской организации сотрудничества, Конвенция Африканского союза и др.). Вместе с тем, сказанное не означает, что в соглашениях первой группы отсутствуют вопросы взаимодействия между государствами, а в договорах второй группы не закрепляется норм материального права.

Наиболее значимым и заслужившим авторитет международным соглашением в рассматриваемой области является Будапештская конвенция Совета Европы 2001 г., регламентирующая порядок осуществления совместных действий, направленных на формирование единой уголовно-правовой политики, которая была бы направлена на обеспечение кибербезопасности. Предполагается, что такая деятельность должна реали-

зовываться через установление преступности и наказуемости соответствующих деяний, а также наделение правоохранительных органов действенными полномочиями, достаточными для их эффективной работы в указанном направлении. От государств-участников Конвенции требуется оказывать максимальное содействие расследованию и судебному рассмотрению преступлений данной группы, причем такое содействие должно быть обеспечено как на внутригосударственном, так и на международном уровнях.

Несмотря на значимость данного международного соглашения, нельзя не отметить, что в нем не содержится самого понятия «киберпреступление». Однако анализ его норм позволил выделить основные признаки, которым данное преступное деяние должно соответствовать. Так, разработчики Конвенции посчитали необходимым обязать государства, ее ратифицировавшие, включить в свое внутреннее уголовное законодательство группу преступлений, посягающих на конфиденциальность, целостность и доступность информации, группу правонарушений, совершение которых предполагает использование компьютерных средств, группу правонарушений, предметом которых выступает специальная информация (медийные материалы, связанные с детской порнографией), а также группу правонарушений, сопряженных с нарушением авторских и смежных прав.

По прошествии непродолжительного времени к данной Конвенции был принят также дополнительный протокол, в котором отдельные противоправные деяния получили специальную регламентацию ввиду их повышенной общественной опасности в связи с возможностью причинения вреда человечеству или значительной его части. Так, дополнительной регламентации подлежали такие правонарушения, как распространение расистских и ксенофобских материалов, угроза расизма и ксенофобии, расистское и ксенофобское оскорбление, одобрение либо оправдание геноцида или иных преступлений против человечества, если такие деяния были совершены с использованием компьютерных систем или сетей.

Таким образом, следует сделать вывод о том, что на сегодняшний день многие нормы, на которых основывается международно-правовая регламентация борьбы с киберпреступностью, в настоящее время утрачивают свою актуальность ввиду стремительного развития технического прогресса, появления новых информационно-коммуникационных средств и систем связи. Актуальность же самой проблемы существования киберпреступлений не только не утрачивается, но с каждым годом все более возрастает. От государств на сегодняшний день требуется более интенсивная работа, направленная на актуализацию существующих

и принятие новых соглашений в рассматриваемой области сотрудничества. В противном случае правового инструментария, имеющегося в распоряжении правоохранительных органов, может оказаться недостаточным для успешной борьбы с возникающими киберугрозами.

Библиографические ссылки

1. Экс-глава генштаба США: в 2015 году «русские хакеры» взломали Пентагон // РИА Новости [Электронный ресурс]. – Режим доступа: <https://ria.ru/20161216/1483758089.html>. – Дата доступа: 29.03.2020.