Секция «Актуальные вопросы современного международного права»

Актуальные проблемы международного права в части преступлений в сфере компьютерной информации

Научный руководитель – Нешатаева Татьяна Николаевна

Аббуд Руслан Ратебович
Аспирант
Российский государственный университет правосудия, Факультет подготовки кадров высшей квалификации, Москва, Россия
E-mail: ruslan625@yandex.ru

На сегодняшний день, с прогрессивным развитием технологий в области компьютерной информации, появляются новые виды киберпреступлений, которые не закреплены на международном уровне.

Киберпреступность представляет собой глобальную угрозу и вызов для всего мирового сообщества. Официальная позиция Российской Федерации заключается в том, что существует проблема международной информационной безопасности. По мнению директора департамента по вопросам новых вызовов и угроз МИД РоссииРогачева И.И. в Российской Федерации международная информационная безопасность включает в себя три элемента:

1) военно - политическая составляющая;

2) экономическая;

3) кибертерроризм, который, в свою очередь, включает две составляющие. Во-первых, это террористические атаки на сети, что, собственно, и понимается как кибербезопасность. Другой аспект, это использование интернета для распространения террористической идеологии, пропаганды терроризма.

В соответствии с Соглашением между Правительствами государств-членов Шанхайской организации сотрудничества о сотрудничестве в области обеспечения международной информационной безопасности,международная информационная безопасность трактуется, как состояние международных отношений, исключающее нарушение мировой стабильности и создание угрозы безопасности государств и мирового сообщества в информационном пространстве.

Российская Федерация и Соединенные Штаты Америки на национальном уровне выработали концепции, которые регламентируют вопросы информационной безопасности. Так, в Российской Федерации принят Указ от 5 декабря 2016 г. № 646 «Об утверждении Доктрины информационной безопасности Российской Федерации». В свою очередь, в Соединенных Штатах Америки действует доктрина о Кибербезопасности (сентябрь, 2018 г.).

На сегодняшний день идет образование системы международной информационной безопасности. Международная информационная безопасность является составной частью системы международной безопасности. Важно отметить тот факт, что международная информационная безопасность служит регулирующим факторомсистемы международных отношений невластного характера. Вместе с тем некоторые угрозы международной информационной безопасности затрагивают область как международных властных, так и не властных отношений.

В 2001 году Советом Европы был разработан и с 2004 года в рамках данной организации действует - Конвенция о преступности в сфере компьютерной информации ETS N 185 (Будапешт, 23 ноября 2001 года) (далее - Конвенция). А также дополнительный протокол к Конвенции по киберпреступлениям в отношении криминализации деяний расистского и

ксенофобского характера, осуществляемых при помощи компьютерных систем (г. Страсбург, 28 января 2003 года).

В настоящее время Конвенция содержит не полный перечень преступлений в сфере компьютерной информации. За время после появления данного соглашения появились новые киберпреступления. В частности, кибербуллинг и кибертерроризм не вошли в перечень преступлений, прописаных в Конвенции.

Трудность в вопросе международно-правового противодействия преступлениям в сфере компьютерной информации усугубляется отсутствием согласованных доктринальных взглядов на природу киберпреступности. Характер нынешнего международного правотворчества в части борьбы с киберпреступностью обусловлен генезисом и определяющими факторами развития преступлений в сфере компьютерной информации.

22 марта 2008 года Президент Российской Федерации подписал распоряжение о признании утратившим силу распоряжение Президента Российской Федерации от 15 ноября 2005 года № 557-рп «О подписании Конвенции о киберпреступности» (далее - распоряжение). Согласно этому распоряжению, Российская Федерация не является участником Конвенции. В частности, Россию не устроил вариант возможного вмешательства зарубежных спецслужб в информационное пространство Российской Федерации без официального уведомления. Это могло бы привести к угрозе национальной безопасности и суверенитету страны.

Кибербуллинг (в Российской Федерации принято говорить Кибертравля или Интернет - травля), представляет собой угрозы, диффамации, намеренные оскорбления и осуществляется в информационном пространстве через информационно-коммуникационные каналы и средства ЭВМ. Стремительное развитие технологий существенно облегчило отправление оскорбительных или угрожающих сообщений в сети «Интернет». В с вязи с тем, что индивиды, в отношении которых было совершенно данное злодеяние не всегда имеют возможность сообщить об этом в компетентные органы, означает, что эти случаи могут остаться латентными. Также существует неясность в отношении того, кто обладает соответствующей юрисдикцией для расследования этого преступления и является ли оно преступлением de jure.

В настоящий момент, в Российской Федерации этот вид преступления в сфере компьютерной информации на законодательном уровне не закреплен. Действующая Конвенция также не содержит положений, регулирующих данный вид киберпреступности.

В Объединенных Арабских Эмиратах на национальном уровне существует Федеральный Закон № 5 от 2012 года о борьбе с киберпреступностью, который содержит положения об оскорблениях в сети «Интеренет» и предусматривает достаточно серьезное наказание в виде реального тюремного срока и депортацией для экспатов. В 2018 году Президент Объединенных Арабских Эмиратов Халифа ибн Зайд аль-Нахайян издал указ о принятии ряда поправок к Федеральному Закону № 5 от 2012 года о борьбе с киберпреступностью, которые в значительной степени смягчили санкции за кибербуллинг. Реальный тюремный срок и обязательная депортации для экспатов заменились на запрет пользоваться «Интернетом» в течение определенного периода времени и денежным штрафом.

На мой взгляд, данный вид правонарушения в сети «Интеренет» можно отнести скорее к административному, чем к уголовному преступлению. Целесообразным видится внесение данного деликта в Кодекс Российской Федерации об административных правонарушениях.

Появление возможности оплачивать покупки онлайн дало возможность киберпреступникам совершать мошеннические махинации в сети «Интернет». Кардеры способны за короткий промежуток времени получить доступ к конфиденциальной информации о финансовой и личной жизни граждан и извлечь крупную прибыль с продажи этих данных.

В деле United States of America (plaintiff) vs Roman V. Seleznev (defendant), 21 апре-

ля 2017 года Окружной Суд Соединенных Штатов по Западному Округу Вашингтона в Сиэтле приговорил к 30 годам тюремного заключения ответчика. К моменту задержания Интерпол оперативно объявил его в международный розыск с пометкой «красное уведомление». Романа Селезнева задержали на Мальдивских островах и затем экстрадировали в США. Спецслужбам США удалось договориться с правоохранительным органами Мальдивских островов, чтобы те помогли с задержанием россиянина, так как договор об экстрадиции между этими государствами отсутствует.

По словам президента Люксембургского форума по предотвращению ядерной катастрофы, Вячеслава Кантора: «киберугрозы уже сейчас непосредственно касаются государственной инфраструктуры ядерных государств и теоретически, у киберзлоумышленников может появиться доступ к ядерному оружию». Не сложно догадаться, что этот глобальный вопрос затронет безопасность всего населения земли и мирового сообщества.

28 декабря 2019 года Генассамблея ООН приняла предложенную Российской Федерацией резолюцию по борьбе с киберперступностью под названием «Противодействие использованию информационно-коммуникационных технологий в преступных целях». Позиция Российской Федерации заключается в том, что резолюция фактически закрепляет цифровой суверенитет государств над своим информационным пространством. Таким образом, возможно, мы скоро станем свидетелями появления новой универсальной международной конвенции, которая воплотит в себе новые преступления в киберпространстве.

В последнее время, в нашей стране, активно обсуждается вопрос искусственного интеллекта на самом высоком уровне. Владимир Владимирович Путин подписал указ от 10.10.2019 № 490 «О развитии искусственного интеллекта В Российской Федерации». В Указе утверждена национальная стратегия по развитию искусственного интеллекта, в которой определены цели и основные задачи развития искусственного интеллекта в Российской Федерации.

С развитием информационных технологий киберзлоумышленники находят новые способы для того, чтобы совершить кибератаки. Транснациональным и неправительственным организациям необходимо своевременно реагировать на возрастающее количество предупреждений систем кибербезопасности.

Могут потребоваться годы обучения для того, чтобы программа искусственного интеллекта была готова к работе в полевых условиях. Киберзлоумышленники создают новые способы взлома корпоративных систем и этопорождает перманентное поступление новых данных о киберпреступниках, которые необходимо регулярно включать в обучение. Модели обучения искусственного интеллекта необходимо будет постоянно обновлять и адаптировать к новым угрозам наряду с разработкой новых стратегий борьбы с ними.

Подводя итоги вышесказанному, стоит отметить, что такой глобальный вызов и угроза, как киберпреступность, требует принятия соответствующих мер, где искусственный интеллект может выступать в качестве основного орудия в борьбе с современными киберугрозами, а также инструментом обеспечения международной информационной безопасности. Благодаря алгоритмам машинного обучения и обработке больших массивов данных, автоматизации процесса выявления и ликвидации опасностей, искусственный интеллект способен обеспечить необходимую киберзащиту. Вместе с тем актуальным и целесообразным видится потребность в необходимости выработки на международном уровне нормативно правового акта универсального характера, который будет регулировать новые преступления в сфере компьютерной информации, а также регламентировать в международном правовом поле «Интернет».

Источники и литература

1) Аббуд Р.Р. Киберхалифат: нормативное определение и криминологическая характеристика в национальном и международном информационном праве // Вопросы российского и международного права. 2018 Том 8 № 8А. С. 190-197.
2) Чернядьева Н.А. – д.ю.н. О международных подходах правового регулирования борьбы с кибертерроризмом. Информационное право. Издательство группа «Юрист». 2016. С 27.
3) Cybercrime and digital forensics: an introduction. (Thomas J. Holt, Adam M. Bossler and Kathryn C. Seigfried-Spellar). 2018, p. 53.
4) UNITED STATES DISTRICT COURT FOR THE WESTERN DISTRICT OF WASHINGTON AT SEATTLE NO. CR11-0070RAJ SENTENCING MEMORANDUM. April 14, 2017
5) Конвенция Совета Европы «О преступности в сфере компьютерной информации» (ETS №185), (Будапешт, 23 ноября 2001 года).
6) Конвенция Совета Европы «О преступности в сфере компьютерной информации» (ETS №185), (Будапешт, 23 ноября 2001 года).
7) Талимончик В.П. Международно-правовое регулирование отношений в сфере информации. Автореф. Дис. на соискание уч. степени д.ю.н. Санкт-Петербург, 2013.-39.
8) Соглашение между Правительствами государств-членов Шанхайской организации сотрудничества о сотрудничестве в области обеспечения международной информационной безопасности.
9) Указ Президента Российской Федерации от 10.10.2019 № 490 «О развитии искусственного интеллекта в Российской Федерации».