Секция «Международная безопасность: новые вызовы и угрозы»

Киберпреступность в России и ЕС: современное состояние, способы борьбы, возможности сотрудничества

Научный руководитель – Энтина Екатерина Геннадьевна

Акимова Алена Андреевна
Студент (бакалавр)
Национальный исследовательский университет «Высшая школа экономики», Факультет мировой экономики и мировой политики, Москва, Россия
E-mail: alyonaakimova@mail.ru

На сегодняшний день киберпреступность является одним из главных препятствий мирового экономического развития. Так, общая стоимость совершенных за 2017 г. киберпреступлений составила 608 млрд. долл. или 0,8% мирового ВВП [10]. Примечательно, что основной целью преступников в онлайн-сфере остаются страны Европы и Центральной Азии, включая Россию - в среднем потери жертв киберпреступлений в этих странах за этот же период были равны 0,89% ВВП [10]. При этом среди таких жертв находятся как частные, так и государственные структуры, которые не только заинтересованы в процессе борьбы с хакерами, но и вовлечены в него. Более того, трансграничный характер таких правонарушений привел к тому, что данная проблема рассматривается и на международном уровне в многостороннем и двустороннем формате, например, между РФ и ЕС. Одной из особенностей такого сотрудничества является общность целей акторов, которая способствует диалогу даже в условиях серьезных политических противоречий.

Тем не менее, на сегодняшний день отсутствует единое понятие киберпреступности и киберпреступлений. Более того, в англоязычной литературе встречаются различные написания этих терминов: “cybercrime”, “cyber-crime”, “cyber crime”. Несмотря на отсутствие международно-правового документа на глобальном уровне, закрепляющего основные положения, касающиеся проблемы киберпреступности и борьбы с ней, многие государства используют в качестве основы Конвенцию о компьютерных преступлениях 2001 г., или Будапештскую конвенцию [8]. В частности, её основные положения в модифицированном виде изложены в Стратегии кибербезопасности ЕС 2013 г. [2], которая является основным современным документом интеграционного образования в сфере защиты данных и информационных систем. Так, к киберпреступности относятся преступления против конфиденциальности, целостности и доступности компьютерных данных и систем (незаконные доступ или перехват, вмешательство в данные или систему и ненадлежащее использование устройств); преступления, связанные с компьютерами (подлог данных и мошенничество); правонарушения, связанные с содержанием (детская порнография) и преступления, связанные с нарушениями авторского права и смежных прав. Россия не является подписантом Будапештской конвенции [9], однако глава 28, а также ст. 146,159.6, 187 УК РФ, регулирующие преступления в сфере компьютерной информации, отображают похожее содержание [6]. Таким образом, РФ и ЕС имеют не единую, но аналогичную правовую основу регулирования киберпреступности.

Чтобы понять приоритеты ЕС и РФ в области борьбы с киберпреступлениями, необходимо проанализировать основные тренды правонарушений в онлайн-сфере. Если рассматривать период с 2013 г., когда была принята Стратегия кибербезопасности ЕС и дополнение к Концепции внешней политики РФ 2013 г. «Основы государственной политики Российской Федерации в области международной информационной безопасности на период до 2020 года», то по 2017 г. тренды киберпреступности в России и ЕС претерпели несколько изменений, при этом они были идентичны. Так, от атак на компьютеры хакеры

перешли к атакам на мобильные устройства, которые приобрели большую популярность [4]. Кроме того, от единичных атак на частные структуры киберпреступники перешли к организованным массовым киберпреступлений против целостности государственных инфраструктур [5]. Тем не менее, финансовая выгода осталась одним из основных приоритетов хакеров в РФ и ЕС. Иными словами, основные вызовы для ЕС и РФ - защита государственной инфраструктуры и финансовых институтов.

Что касается институционального регулирования, то российский и европейский подход значительно отличаются. Прежде всего, ЕС уделяет большее внимание частному сектору и партнерству с ним. Более того, для расследования киберпреступлений привлекаются российские ИТ-компании, например, Лаборатория Касперского и Group-IB [7]. Основой же борьбы и управления вопросами киберпреступности в ЕС является агентство ENISA, а также специальное подразделение EC3 в Европоле [3]. Российский подход также основан на создании специального отделения в рамках МВД - «Управления К» - однако в отличие от ЕС оно не привлекает частный сектор и не раскрывает информацию публично, что, по мнению многих исследователей, мешает сотрудничеству [1]. Тем не менее, ЕС и РФ также используют и другие каналы, например, Интерпол для взаимодействия и передачи информации, что является важнейшим положением для борьбы с киберпреступлениями.

Подводя итог вышесказанному, на сегодняшний день киберпреступность представляет собой один из основных вызовов международной безопасности и стабильности. Однако, одновременно он заставляет акторов искать способы сотрудничества даже в условиях кризисных отношений. Основой такого взаимодействия между РФ и ЕС является похожая правовая база, единые тренды киберпреступлений и институциональное взаимодействие через привлечение частного сектора.

Источники и литература

1) Евдокимов К.Н. Противодействие компьютерной преступности в Российской Федерации: криминологические и уголовно-правовые аспекты. Иркутск, 2016
2) Cybersecurity Strategy of the European Union: An Open, Safe and Secure Cyberspace. Brussels, 2013.
3) Christou G. Cybersecurity in the European Union. London, 2016.
4) EUROPOL. IOCTA 2016. Brussels, 2016.
5) Hi-tech crime trends 2017. Отчет Group-IB. Москва, 2017.
6) Консультант Плюс: Уголовный Кодекс Российской Федерации: http://www.consultant.ru/cons/cgi/online.cgi?req=doc&base=LAW&n=291258&fld=134&dst=1000000001,0&rnd=0.4853925719789074#09265050819278886
7) «Лаборатория Касперского» и бельгийская полиция «обезоружили» шифровальщика: http://safe.cnews.ru/news/line/2018-02-09_laboratoriya_kasperskogo_i_belgijskaya_politsiya
8) Совет Европы: Полный список: Подробная информация о Договоре №185: https://www.coe.int/ru/web/conventions/full-list/-/conventions/rms/0900001680081580
9) Совет Европы: Таблица подписей и ратификации договора 185: https://www.coe.int/ru/web/conventions/full-list/-/conventions/treaty/185/signatures?p_auth=JAnp2ozU
10) Lewis J. Economic Impact of Cybercrime — No Slowing Down: https://csis-prod.s3.amazonaws.com/s3fs-public/publication/economic-impact-cybercrime.pdf?kab1HywrewRzH17N9wuE24soo1IdhuHdutm_source=Pressutm_campaign=bb9303ae70-EMAIL_CAMPAIGN_2018_02_21utm_medium=emailutm_term=0_7623d157be-bb9303ae70-194093869