Гуспарян Гурген
Gasparyan Gurgen
Научный руководитель: д.ю.н., доцент **Гаврилин Ю.В.**
Supervisor: Dr. of Law, Associate Professor **Yu.V. Gavrilin**
Адъюнкт Академии управления МВД России
PhD student The Academy of management of the interior Ministry of Russia

Борьба с преступностью в сфере информационных технологий посредством их предупреждения, распространения информации и повышения осведомленности
Combating crime in information technology through prevention, dissemination and awareness-raising

The article is devoted to the fight against crimes in the field of information technology by preventing their Commission, propaganda activities, as well as national and international cooperation. The existing problems in this sphere are considered.

Key words: cybercrime, information technology, crime prevention.

Статья посвящена вопросу борьбы с преступлениями в сфере информационных технологий посредством предотвращения их совершения, пропагандисткой деятельности, а также вопросам национального и международного сотрудничества. Рассмотрены имеющиеся проблемы в данной сфере.

Ключевые слова: киберпреступления, информационные технологии, предотвращение преступлений.

Обычно повторяющееся утверждение относительно Интернета заключается в том, что он быстро развивается и что киберпреступники пользуются всеми возможными преимуществами этого процесса. "Мантра", которая часто следует, заключается в том, что этот темп развития создаёт серьезные проблемы для законодателей, которые должны попытаться догнать эти постоянно развивающиеся явления.

По данным Международного союза электросвязи (МСЭ), специализированного агентства по информационно-коммуникационным технологиям ООН, в 2010 году более 62 млн жителей России регулярно пользовались Интернетом. К концу 2016 года количество пользователей составило 110 млн, что соответствует 76.2 % населения России. Распространение мобильной широкополосной связи также продолжает расти и к концу 2017 года составило свыше 227 млн абонентов.

Фрагментация на международном уровне и разнообразие национального законодательства в области борьбы с преступностью, совершённой с использованием информационных технологий, привели к тому, что в последние годы было обнародовано множество документов, в том числе международных по вопросам борьбы с указанными преступлениями, в частности Конвенция Совета Европы «О киберпреступности» 2001 года [150], Директива ЕС «О нападениях на информационные системы» 2013 года, однако четкой, всеобъемлющей и согласованной рамочной основы по-прежнему не хватает. Наконец, еще одним ключевым фактором является восприятие “низкого риска”, связанного с преступлениями в сфере информационных технологий ввиду их большой латентности[151].

150 Россия в настоящее время не подписала конвенцию. Распоряжение Президента РФ от 22.03.2008 №144-рп "О признании утратившим силу распоряжения Президента Российской Федерации от 15 ноября 2005 г. №557-рп "О подписании Конвенции о киберпреступности"

151 По данным исследования 2013, проводимого управлением ООН по наркотикам и преступности (ЮНОДК), в участвующих странах было подсчитано, что количество зарегистрированных киберпреступлений в полицию по заявлениям потерпевших было в пределах чуть более 1 процента. См. электронный ресурс:

Правовые меры, безусловно, играют жизненно важную роль в борьбе с преступностью в сфере информационных технологий и должны охватывать различные области, начиная от материального аспекта и заканчивая уголовно-процессуальным правом, а также вопросы юрисдикции.

Наряду с этим, представляется, что необходимо уделять должное внимание трем вопросам: профилактике путём оценки угроз, информационно-пропагандистской деятельности и повышению осведомлённости.

Стратегическая разведка и анализ, жизненно важны в ходе борьбы с преступностью в сфере информационных технологий. В методологическом плане речь идет главным образом о сборе данных, их толковании и моделировании будущих событий, тенденций, угроз и возможностей. Стратегическая разведка, применяемая к указанным преступлениям должна дать ответ на вопрос: "Что мы можем сказать о нынешних и будущих угрозах на практическом уровне?".

28.02.2017 года Европол принял довольно структурированную методологию стратегического анализа особенностей организованной преступности (SOCTA)[152]. Данная методология, разработанная для анализа угрозы, создаваемой организованными преступными группами, может быть использована с учетом соответствующих различий для изучения специфики угроз преступлений в сфере информационных технологий.

Интернет сделал географические соображения практически не актуальными, ввиду чего необходимо, чтобы правоохранительные органы взаимодействовали как с государственными, так и с частными заинтересованными структурами, возможно через создание координационного центра.

В рамках ЕС эту роль выполняет Европейский центр по борьбе с Киберпреступностью (ЕСЗ), который, после его основания в январе 2013 года является коллективным органом ЕС в борьбе с киберпреступностью. ЕСЗ поддерживает операции, активно участвует в исследованиях, обучении сотрудников и профилактике преступлений, а также регулярно поддерживать связь с рядом учреждений и органов ЕС. Схожая инициатива предпринята 20.07.2018 по результатам заседания Совета министров внутренних дел стран СНГ, в ходе которого запланировано открытие в России дополнительного учебного заведения для подготовки сотрудников для органов внутренних дел стран Содружества[153].

В борьбе с преступностью в сфере информационных технологий крайне важное значение имеет укрепление доверия между Интернет-отраслью и правоохранительными органами государства.

Также имеет большое значение просвещение пользователей Интернета о том, как лучше всего использовать технологии. Борьба с преступлениями в сфере информационных технологий - это не прерогатива, которая ложится на правоохранительные органы в одиночку.

Национальные правительства должны запустить рекламные кампании, чтобы помочь людям защитить себя от подобных преступлений. Простые меры безопасности, особенно среди молодежи, могут значительно снизить уровень преступности. Повышение осведомленности через систематические кампании средств массовой информации, социальных сетей, является лишь одним из вариантов достижения этой цели.

Помимо повышения уровня информированности широкой общественности, также необходимо приобретение адекватных навыков правоприменителями для борьбы с вышеуказанной преступностью, в связи с чем необходимо внедрение программ подготовки

---

http://www.unodc.org/documents/organized-rime/UNODC_CCPCJ_EG.4_2013/CYBERCRIME_STUDY_210213.pdf. С. 117. Дата обращения 10.10.2018

[152] Электронный ресурс: https://www.europol.europa.eu/activities-services/main-reports/european-union-serious-and-organised-crime-threat-assessment-2017. Дата обращения 10.10.2018

[153] Электронный ресурс: https://www.e-cis.info/page.php?id=26336. Дата обращения 10.10.2018

специалистов на трех различных уровнях: 1) начальные курсы (предлагая базовые знания и понимание преступлений в сфере информационных технологий, риски, связанные с информационно-коммуникационными технологиями, тенденции в данной области, виды рассматриваемых преступлений и основные используемые инструменты, правовые проблемы на национальном и международном уровне); 2) курсы следователей (выявление преступлений, методика расследование компьютерных преступлений, тактика проведения отдельных следственных действий) и 3) курсы для специалистов судебно-экспертной деятельности (более углубленные научные знания по разрешению технических вопросов, продуктов, аналитических процедур, для выполняя роли эксперта в ходе расследовании и судебного разбирательства).

Однако борьба с преступлениями в сфере информационных технологий требует комплексного подхода, который должен учитывать прогноз их тенденций, дабы не допустить новых угроз и заранее обеспечить адекватную подготовку. Профилактика должна сопровождаться информационно-пропагандистским подходом. Правоохранительным органам необходимо наладить диалог на вертикальном уровне (с прокурорами и судьями) и на горизонтальном уровне (с интернет-индустрией, с другими заинтересованными сторонами и гражданским обществом в целом). Повышение общей осведомленности об угрозе преступлений в сфере информационных технологий, избегая при этом подрыва доверия пользователей Интернета, сосредоточив внимание исключительно на потенциальных опасностях, связанных с использованием Интернета, остается ключевой задачей на предстоящие годы.