Грязнов Сергей Александрович
канд. пед. наук, доцент, декан
ФКОУ ВО «Самарский юридический институт ФСИН России»
г. Самара, Самарская область

О НОВОЙ ЦИФРОВОЙ ТИПОЛОГИИ ОРГАНИЗОВАННЫХ ПРЕСТУПНЫХ СЕТЕЙ

Аннотация: *цифровое общество меняет деятельность организованной преступности и преступных группировок: онлайн-киберпреступность, традиционные и гибридные преступные группировки. Автор вносит предложение о создании новой криминологической интерпретационной теоретической основы (определение организованной преступности цифровых сетей), учитывающей изменения, которые цифровое общество вносит в деятельность организованной преступности, и которые способны генерировать более современные исследовательские гипотезы.*

Ключевые слова*: организованная преступность, цифровое общество, цифровые технологии, киберпреступность, ботнет, организованные преступные сети.*

Сегодня миллиарды людей и компаний по всему миру подключены к сети Интернет, где они делают заметки, фотографируют, публикуют информацию, принимают решения. В виртуальном пространстве остаются терабайты цифровой информации, собранной, каталогизированной, помеченной временем и местом, а также другими метатегами. Современные концепции общества и культуры невозможно полностью понять без признания того, что люди, отношения и социальные институты формируются как программными, так и аппаратными устройствами. Цифровые технологии теперь являются неотъемлемой частью того, что значит быть человеком, также предполагая тесное взаимодействие между людьми и машиной. Концепция, используемая для описания гибридных явлений, возникающих в результате взаимодействия между людьми и нечелове-

ческими акторами, представляет собой социотехническую или социоматериальную сборку: все меньше социальных действий осуществляется без использования материальных инструментов. Социоматериальная сборка – это сложные социальные, экономические и технологические отношения между людьми и нечеловеческими субъектами.

Преступления в цифровом обществе меняются с точки зрения типологий и способов действия, а преступники меняются с точки зрения своих характеристик, социальных взаимодействий и отношений с потенциальными жертвами. Там, где появляются новые социальные факты, новые привычки, новые способы покупать, платить, защищать, передавать активы, появляются новые цифровые личности, системы сбора информации. При этом организованная преступность, согласно принципам рациональности, всегда стремиться воспользоваться новыми возможностями, максимизировать прибыль и минимизировать риски [1].

Киберзависимая организованная преступность – это высокотехнологичная организованная деятельность, которая совершается с использованием компьютеров, компьютерных сетей или других форм информационных и коммуникационных технологий и включает в себя взлом, несанкционированный доступ к компьютерным сетям, сотовым телефонам и планшетным устройствам, использование уязвимостей безопасности для сбора личных данных или полезной информации, а также для порчи веб-сайтов и запуска DoS- или DDoS-атак. Второе направление преступной деятельности включает распространение вредоносного ПО (программное обеспечение), которое вмешивается в работу компьютеров и может принимать различные формы, например, вирусы, черви, трояны, шпионские программы, программы-вымогатели; спам (нежелательные сообщения электронной почты, которые обычно рассылаются бесчисленному количеству получателей с целью сбора личной информации; отказ в обслуживании (DoS) (атака, целью которой является вывести компьютер или сеть из строя, наводнив его нежелательным интернет-трафиком или отправив ему информацию, которая может привести к его сбою).

Мир мошенничества входит в число областей, которые больше всего выиграли от появления сети Интернет. Цифровое общество «индустриализовало» масштабы мошенничества точно так же, как современные технологии расширили возможности бизнеса по выходу на более крупные и прибыльные рынки. Одним из примеров организованного онлайн-мошенничества, которое становится все более распространенным во всем мире является BEC (компрометация деловой электронной почты). В схемах BEC преступники используют хакерство или социальную инженерию для получения соответствующей корпоративной информации, которую они затем используют для обмана руководителей, финансовых директоров и владельцев бизнеса, побуждая их к совершению незаконных платежей от имени компаний [2].

Офлайновая преступная деятельность, которая с точки зрения уголовного правосудия представляет собой взаимозависимые «цепочки» преступлений, которым способствует использование компьютеров, компьютерных сетей или других форм информационных и коммуникационных технологий. Здесь цифровой инструмент не имеет решающего значения – его роль второстепенная, хотя и важная (сеть Интернет используется для поддержки организации и ее деятельности). Таким образом, под формами преступлений с использованием кибербезопасности подразумевается сложная преступная деятельность, совершаемая преступными группами или отдельными лицами, которые используют технологии для поддержки уже существующих преступных операций.

Возникает вопрос, являются ли киберпреступные группы организованной преступностью в традиционном смысле? Для существования организованной преступности, помимо преступного сообщества, необходимы: совершение тяжких преступлений, продолжительность и стабильность во времени, а также другие элементы, такие как применение насилия, коррупция и возможность проникновения в экономику. Следовательно, сложно провести аналогии между группами киберпреступников, действующими исключительно в сети Интернет и традиционной организованной преступностью. Элементы традиционной «мафиоз-

ной» организованной преступности в киберпреступных группировках встречаются редко и практически никогда не появляются в сетевых преступных организациях, потому что организация (организованной) киберпреступности следует логике, отличной от логики традиционной организованной преступности. Это «дезорганизованная» модель: группы киберпреступников основаны на репутационной динамике, состоят из малого числа лиц и часто не имеют иерархической структуры управления. В отличие от традиционных преступных организаций, члены онлайн-преступной организации могут никогда не встречаться.

Чтобы лучше понять текущие события в цифровом обществе, следует также учитывать новые формы организованной преступности, которые пока кажутся футуристическими. Ботнеты – сети зараженных компьютеров, контролируемых одним или несколькими контроллерами для проведения кибератак, и которые все чаще используются для киберпреступлений. Таким образом, стандартное определение организованной преступности, основанное на участии трех или более лиц, действующих согласованно, не распространяется на некоторые весьма сложные формы организации, такие как мобилизация роботизированных сетей, которыми может управлять один человек. В так называемых ботнетах злоумышленник использует вредоносное программное обеспечение для получения контроля над большим количеством компьютеров (крупнейший из которых включает более миллиона отдельных компьютеров). Несмотря на то, что отдельные и институциональные хранители взломанных компьютеров могут быть невольными участниками преступного предприятия, бот-сети, мобилизованные единственным преступником, следует рассматривать как форму организованной преступности.

В контексте ботнетов введен термин «киборг-преступление» (правонарушение акторов, которые не являются ни полностью людьми, ни полностью машинами). Если использовать антропоцентрическую криминологию, которая рассматривает людей как единственную движущую силу преступной деятельности, невозможно понять природу преступлений, совершаемых через бот-сети. Это

приводит к выводу, что существует совершенно новая форма гибридной организованной преступности, где взаимодействие между людьми и нечеловеческими существами настолько глубоко, что следует подумать о новой цифровой типологии организованных преступных сетей [3].

Обсуждения киберпреступности и организованной преступности в целом наполнены стереотипами. С одной стороны, образ «одинокого хакера» противоречит коллективному характеру многих киберпреступлений. С другой стороны, общепринятые определения организованной преступности имеют тенденцию устаревать, поскольку их вытеснила эволюция самого этого явления. Нужен новый теоретический подход, позволяющий уловить чрезвычайную сложность и нюансы организации преступных группировок и преступной деятельности в цифровом обществе, а также новшества, которые цифровое общество привносит в субъективные и объективные элементы организованной преступности.

Список литературы

1. Пырчев С.В. Тенденции организованной преступности в развивающемся цифровом мире / С.В. Пырчев // Труды Академии управления МВД России. – 2020. – №2 (54) [Электронный ресурс]. – Режим доступа: https://cyberleninka.ru/article/n/tendentsii-organizovannoy-prestupnosti-v-razvivayuschemsya-tsifrovom-mire (дата обращения: 03.06.2024).

2. Дрозд А. Компрометация почты: как защитить бизнес от BEC-атаки / А. Дрозд [Электронный ресурс]. – Режим доступа: https://globalcio.ru/discussion/32500/ (дата обращения: 03.06.2024).

3. Белов Д.Ю. Современные методы защиты от кибератак / Д.Ю. Белов [Электронный ресурс]. – Режим доступа: https://www.elibrary.ru/item.asp?id=46352256 (дата обращения: 03.06.2024).