

*Носова Дарья Игоревна, студент  
ФГБОУ ВО «Саратовская государственная юридическая академия»  
Институт магистратуры и заочного обучения  
Научный руководитель: Вишневецкая Ирина Николаевна  
доцент, кандидат юридических наук,  
доцент кафедры прокурорского надзора и криминологии  
ФГБОУ ВО «Саратовская государственная юридическая академия»*

**СОВРЕМЕННЫЕ ИНФОРМАЦИОННО-ТЕХНОЛОГИЧЕСКИЕ  
(ЦИФРОВЫЕ) МЕРЫ ПРЕДУПРЕЖДЕНИЯ ОРГАНИЗОВАННОЙ  
ПРЕСТУПНОСТИ**

***Аннотация:** В статье отображается проблематика предупреждения организованной преступности в условиях развития информационного (цифрового) пространства. Анализируются способы совершения организованной преступной деятельности в сфере высоких технологий и предлагаются меры по их предупреждению. Основное внимание уделяется использованию преступниками информационных технологий для совершения противоправных деяний, а также необходимости внедрения современных информационно-технологических мер в деятельность правоохранительных органов.*

***Abstract:** The article highlights the problems of preventing organized crime in the context of the development of the information (digital) space. It also analyzes the ways of committing organized criminal activities in the field of high technology and suggests measures to prevent them. The main focus is on the use of information technology by criminals to commit illegal acts, as well as the need to introduce modern information technology measures into the activities of law enforcement agencies.*

*Ключевые слова:* организованная преступность, информационно-технологические (цифровые) меры предупреждения организованной преступности.

*Keywords:* organized crime, information technology (digital) measures to prevent organized crime.

Политика по предупреждению организованной преступности на территории государства видоизменяется в зависимости от того, какие криминогенные признаки на сегодняшний день преобладают, и какая преступная обстановка складывается на сегодняшний день. Различные меры предупреждения организованной преступности, позволяют минимизировать показатели противоправных деяний на территории государства, а также позволяют бороться с причинами и условиями совершения преступлений. Целью внедрения мер по предупреждению организованной преступности является сокращение числа преступных посягательств. В научной литературе и на законодательном уровне разработаны различные методы и меры по предупреждению организованной преступности, к которым следует отнести: общее предупреждение организованной преступности; специальное предупреждение организованной преступности; индивидуальное предупреждение организованной преступности.

Важное значение в предупреждении организованной преступности имеют меры специально-криминологического предупреждения преступности, под которыми следует понимать совокупность мероприятий, направленных на выявление и устранение причин и условий организованной преступности и всей преступности в целом, на лиц, совершающих преступные деяния, и их жертв. Так, одним из детерминантов организованной преступности является развитие использования преступниками информационных (цифровых) технологий для достижения целей и задач совершения противоправных деяний. В течение последних десятилетий, информационное пространство

Российской Федерации испытывает многочисленные изменения, которые обуславливаются разнообразием информационных источников.

Информационные технологии неразрывно связаны с информационной безопасностью в обществе, в частности, меры по созданию и поддержанию информационной безопасности направлены на защиту национальных интересов, защиту личности и общества при получении, распространении, использовании информации. По данным МВД РФ, в 2024 году в России доля преступлений в сфере ИТ (при помощи информационно-телекоммуникационных технологий) составила 40% от общего числа зарегистрированных в стране. Это наивысший показатель с 2020 года<sup>1</sup>.

При совершении организованных преступлений, нарушаются не только права и интересы человека и гражданина, но и также общества и государства в целом. В связи с тем, что развитие информационного общества влияет не только на усовершенствование различных процессов в обществе, но и на усовершенствование способов и методов совершения противоправных деяний, то целесообразнее рассмотреть (предложить) современные информационно-технологические (цифровые) меры предупреждения организованной преступности. Влияние информационных технологий на организованную преступность проявляется в следующих аспектах:

- Расширение незаконных рынков и сетей;
- Развитие новых видов организованной преступности;
- Изменение способа структурирования и организации преступных групп;
- Увеличение объёмов, скорости и закрытости международных финансовых расчетов.

---

<sup>1</sup> По данным МВД РФ, в 2024 году в России доля преступлений в сфере ИТ (при помощи информационно-телекоммуникационных технологий) составила 40% от общего числа зарегистрированных в стране. Это наивысший показатель с 2020 года. // Медиагруппа «Звезда». URL: <https://tvzvezda.ru/news/2025127612-5N15E.html> (дата обращения: 23.04.2025).

Организованные группировки (сообщества) используют современные информационные (цифровые) технологии в качестве инструмента для повышения эффективности противоправной деятельности и устранения препятствий при совершении противоправных деяний. Отмечается, что преступления, которые совершаются организованными преступными группировками с использованием современных информационных технологий, подразделяются на две большие группы:

- Преступления ненасильственного характера (например, отмывание денег, добытых преступным путем; хищение денежных средств с банковских карт; фальшивомонечество; распространение наркотических средств и психотропных веществ торговля огнестрельным оружием);
- Преступления насильственного характера (например, «кибертерроризм», торговля людьми).

Организованная преступность, на современном этапе развития, с помощью использования современных (цифровых) технологий расширяет рамки незаконного оборота цифровых активов на территории Российской Федерации. Так, на территории Российской Федерации существуют псевдо - холдинги и инвестиционные площадки, которые нелегально реализовывают свою деятельность, предлагая инвесторам предоставлять свои цифровые активы в доверительное управление с целью приумножения средств за счет торговли на рынке и бонусной системы поощрений (схема Понци)<sup>2</sup>.

Интернет-пространство на сегодняшний день стало неким механизмом для совершения противоправных деяний организованными группировками (сообществами), поскольку принимая цифровые решения, которые облегчают коммуникацию, используются такие новые информационные (цифровые)

---

<sup>2</sup> Пинкевич, Т.В. Трансформация организованной преступности в условиях цифровизации // Право и управление. - 2023. - №10. - С. 465.

технологии как: закрытые группы или мессенджеры, виртуальные частные сети, анонимные браузеры<sup>3</sup>.

Например, одним из направлений деятельности организованной преступности является торговля людьми. Обращаясь к статистическим данным Глобального индекса рабства, опубликованными в 2024 году, самый высокий уровень распространения торговли людьми наблюдается в следующих странах: Северная Корея, Саудовская Аравия, Турция, Таджикистан, Российская Федерация, Афганистан<sup>4</sup>. Организованные группировки (сообщества), осуществляя свой преступный умысел, например, могут использовать различные форумы, где можно найти сведения о способах доступа к запрещенному контенту; социальные сети (Facebook, Instagram, ВКонтакте и другие); файлообменные сервисы (Яндекс Диск, Google Drive, DropMeFiles и другие). То есть, организованные группировки (сообщества), используя вышеуказанные информационные (цифровые) технологии, скрывают не только противоправные деяния, но и продолжают популяризировать организованную преступность с помощью внедрения в свою деятельность таких технологий.

Большую опасность, и одновременно сложность в процессе поиска и предупреждения организованной преступности представляет та организованная преступность, которая осуществляет свой преступный умысел посредством распространения запрещённого контента в сети Darknet<sup>5</sup>. Сеть Darknet – это та сеть, где сайты и пользователей практически невозможно отследить по причине того, что вся информация о них, в том числе местоположение, надежно скрывается с помощью сети Tor. Следовательно, при развитии сети Darknet, как способе осуществления преступного умысла,

---

<sup>3</sup> Теуважуков, А.Х. Цифровые технологии в арсенале организованной преступности // Право и управление. - 2024. - №6. - С. 360.

<sup>4</sup> Показатели торговли людьми по странам // Официальный сайт Глобального индекса рабства. URL: [https://translated.turbopages.org/proxy\\_u/en-ru.ru.e546d0b0-6835d3c3-b3891600-74722d776562/https/worldpopulationreview.com/country-rankings/human-trafficking-rates-by-country?](https://translated.turbopages.org/proxy_u/en-ru.ru.e546d0b0-6835d3c3-b3891600-74722d776562/https/worldpopulationreview.com/country-rankings/human-trafficking-rates-by-country?) (дата обращения: 27.05.2025).

<sup>5</sup> Бутраменко, В. Д. Торговля людьми и интернет: как это связано? // Молодой ученый. - 2019. - № 31 (269). - С. 92.

на территории государства должны быть введены меры по предотвращению и предупреждению совершения таких противоправных деяний.

Так, для предотвращения развития сети Darknet, правоохранительными органами на постоянной основе блокируются (ликвидируются) интернет-ресурсы, с помощью которых осуществляется противоправная деятельность организованных группировок (сообществ). При этом проблемной стороной, именно в предупреждение правоохранительными органами организованной преступности в сфере использования современных информационных (цифровых) технологий, является то, что правоохранительные органы не снабжены техническими возможностями, которые бы позволяли на первоначальном этапе пресекать данный вид преступности в информационном пространстве<sup>6</sup>.

Таким образом, для избежания формирования нового вида организованной преступности с использованием информационно-технологических способов совершения противоправных деяний, необходимо внедрить в деятельность правоохранительных органов современные информационно-технологические (цифровые) меры по их предупреждению, а именно, внедрить информационные платформы в деятельность правоохранительных органов, позволяющие идентифицировать развитие незаконной деятельности в сети Darknet и в других информационных (цифровых) пространствах.

Проблемной стороной в разработке информационно-технологических (цифровых) мер по предупреждению организованной преступности является то, что такие меры затрагивают только такие способы как: распространение информации, усовершенствование правовых систем, подготовка и постоянное повышение квалификации работников правоохранительной системы. Данные меры, указанные выше, имеют место быть, однако, ранее были определены

---

<sup>6</sup> Григорян, Д.К. Криминальные противостояния Даркнета и правовых институтов государственной власти // Философия права. - 2022. - №3 (102). - С. 140.

информационно-технологические инструменты, с помощью которых организованная преступность осуществляет незаконную деятельность, следовательно, меры предупреждения данного вида преступлений, должны также быть направлены не только на причины и условия их совершения, но и на способы совершения данных противоправных деяний.

Иными словами, современные информационно-технологические (цифровые) меры по предупреждению организованной преступности в рамках развития информационного общества должны предусматривать следующие аспекты:

- Внедрение автоматизированной системы выявления нарушений при создании и использовании интернет-платформ на территории Российской Федерации;
- Внедрение автоматизированной платформы, осуществляющей постоянный контроль за распространением незаконной информации в сети Интернет;
- Рассмотрение вопроса об использовании информационных систем (платформ) в правоохранительных органах, чья деятельность направлена на предупреждение преступности;
- Разработка пособий для правоохранительных органов, осуществляющих предупреждения организованной преступности, с включением важных аспектов рассмотрения использования такими группировками информационных (цифровых) технологий.

Таким образом, невозможно не отметить влияние современных тенденций развития информационной сферы общества на формирование новых способов совершения преступлений. Одним из многочисленных направлений развития информационного общества является организационно-правовые механизмы анализа защищенности цифровых данных, а также формирования безопасной цифровой среды в государственных органах

власти, что в дальнейшем будет отображаться на эффективном предупреждении организованной преступности.

### Список использованной литературы

1. Бутраменко, В. Д. Торговля людьми и интернет: как это связано? // Молодой ученый. - 2019. - № 31 (269). - С. 91-93.
2. Григорян, Д.К. Криминальные противостояния Даркнета и правовых институтов государственной власти // Философия права. - 2022. - №3 (102). - С. 138-146.
3. По данным МВД РФ, в 2024 году в России доля преступлений в сфере IT (при помощи информационно-телекоммуникационных технологий) составила 40% от общего числа зарегистрированных в стране. Это наивысший показатель с 2020 года. // Медиагруппа «Звезда». URL: <https://tvzvezda.ru/news/2025127612-5NI5E.html> (дата обращения: 23.04.2025).
4. Пинкевич, Т.В. Трансформация организованной преступности в условиях цифровизации // Право и управление. - 2023. - №10. - С. 464-470.
5. Показатели торговли людьми по странам // Официальный сайт Глобального индекса рабства. URL: [https://translated.turbopages.org/proxy\\_u/en-ru.ru.e546d0b0-6835d3c3-b3891600-74722d776562/https/worldpopulationreview.com/country-rankings/human-trafficking-rates-by-country?](https://translated.turbopages.org/proxy_u/en-ru.ru.e546d0b0-6835d3c3-b3891600-74722d776562/https/worldpopulationreview.com/country-rankings/human-trafficking-rates-by-country?) (дата обращения: 27.05.2025).
6. Теуважуков, А.Х. Цифровые технологии в арсенале организованной преступности // Право и управление. - 2024. - №6. - С. 358-362.