

Секция «Обеспечение финансовой безопасности России: финансовые расследования в цифровой экономике»

## Противодействие «Даркнету» в контексте обеспечения финансовой безопасности Российской Федерации

Научный руководитель – Хабибулин Алик Галимзянович

*Федорович Михаил Александрович*

*Студент (бакалавр)*

Московский государственный университет имени М.В.Ломоносова, Высшая школа государственного аудита, Кафедра экономических и финансовых расследований, Москва, Россия

*E-mail: mi.major@yandex.ru*

Начиная с середины XX века традиционные представления об информации претерпевают постоянные изменения. Одной из ключевых причин происходящих метаморфоз стало создание интернета. Его появление парадигмально изменило общемировую действительность, привнеся наряду с положительными (позитивными) последствиями и негативные, включая угрозы финансовой безопасности.

Неотъемлемой частью этих угроз являются компьютерные преступления (фишинг, ферминг, использование RFID, руткитов, кейлоггеров, троянов и т.д.) [1], которые охватываются главой 28 «О преступлениях в сфере компьютерной информации» Уголовного кодекса Российской Федерации (далее - УК РФ). Однако наибольший интерес представляет другая группа преступлений, которую можно подразделить на две составляющие. В первую очередь - это уголовные правонарушения, которые совершаются в интернете, но без использования специальных средств и такие, для доступа к которым нужны особые алгоритмы, программы и оборудование, то есть, в «Даркнете» - части информационно-телекоммуникационного пространства, характеризующейся тремя признаками:

- 1) Шифрование соединения;
- 2) Анонимность - сокрытие реального IP-адреса пользователя;
- 3) Информация, передаваемая в «Даркнете» носит запрещенный, в зависимости от юрисдикции, характер.

Для самого соединения важны первые два критерия, третий же позволяет отделить просто анонимный сегмент от преступного[2].

В силу того, что широкое распространение «Даркнет» получил всего несколько лет назад, на сегодняшний день в России не сформированы эффективные механизмы по рациональному противостоянию данной угрозе. Основными способами являются следующие:

- Блокирование ресурса с выявлением лиц, причастных к его созданию [3,4]
- Внедрение правоохранительных органов в организационную структуру «Даркнета»;
- Отслеживание платежных операций с криптовалютой [6];
- Дешифрование механизмов, используемых для доступа в «Даркнет»[5];

Резюмируя все выше сказанное, следует констатировать недооцененность «Даркнета» как угрозы финансовой безопасности в Российской Федерации, а также отсутствие эффективного механизма противодействия «Даркнету». В этой связи хотелось бы предложить следующие меры по предотвращению, профилактике и недопущению угроз финансовой безопасности, формируемых на основе «Даркнета»:

- 1) Подготовка специалистов в области экономической и финансовой безопасности;
- 2) Создание нормативно-правовой базы, где будет регламентирован статус «Даркнета» и всех сопутствующих явлений (например, криптовалюты, шифрующих приложений);
- 3) Построение эффективного механизма взаимодействия государственных органов, обеспечивающих финансовую безопасность и частных организаций, специализирующихся на безопасности информационных систем;
- 4) Построение эффективного межгосударственного взаимодействия в области предотвращения угроз, формируемых «Даркнетом»;
- 5) Формирование культуры пользования сетевыми ресурсами и цифровыми технологиями в целях предупреждения девиации личности;
- 6) Особый контроль за банковскими и парабанковскими организациями, предоставляющими услуги по обмену криптовалют.

#### Источники и литература

- 1) Сомик К. В., Хабибулин А. Г. Под общей редакцией Шахрая С. М. Информационно-аналитическое обеспечение финансовых расследований. Москва, АРГАМАК-МЕДИА, 2017
- 2) Федорович М. А. Темный интернет в системе интернет-преступности // научный электронный журнал «Меридиан», 2020 Выпуск №7
- 3) Официальный сайт МВД РФ: <https://xn-b1aew.xn-p1ai/news/item/18923122/>
- 4) Официальный сайт ЦОС ФСБ РФ: <http://www.fsb.ru/fsb/press/message/single.htm%21id%3D10438525%40fsbMessage.html>
- 5) CNN: <https://www.cnn.com/2013/12/17/justice/massachusetts-harvard-hoax/index.html>
- 6) Forbes: <https://www.forbes.com/sites/kellyphillipserb/2019/10/16/irs-followed-bitcoin-transactions-resulting-in-takedown-of-the-largest-child-exploitation-site-on-the-web/#91b9ad81ed0d>