Proceedings of International Scientific Conference on Multidisciplinary Studies
Hosted online from Moscow, Russia
Date: 11th June - 2024
ISSN: 2835-5733 **Website:** econferenceseries.com

ПРОБЛЕМЫ БОРЬБЫ С ПРЕСТУПНОСТЬЮ В СКРЫТОЙ СЕТИ DARKNET

Очилов Асадбек Баходир угли
Магистр в академии правоохранительных органов Республики Узбекистан
https://orcid.org/0009-0009-5836-7837

Аннотация:
Данная статья посвящена актуальной проблеме значительного увеличения доли преступлений, совершаемых с использованием информационно-коммуникационных технологий. Основная цель исследования - усовершенствовать методы анализа и оценки преступлений, совершаемых с использованием информационно-коммуникационных систем, и выработать рекомендации, основанные на научных данных. В статье рассматриваются основные методы и механизмы обеспечения информационной безопасности (анонимности в Интернете), а также перспективные методики деанонимизации пользователей, которые могут быть использованы в процессе выявления и раскрытия преступлений. Автор предлагают базовую модель преступности, предназначенную для первичного изучения криминальных личностей. Также предложена методика оценки потенциала информационно-коммуникационных сетей с учетом специфики использования компьютерных средств в преступной деятельности.

Ключевые слова: Даркнет, преступность, методы деанонимизации, модель злоумышленника, раскрытие преступлений, анонимность, информационно-телекоммуникационные сети, теневой Интернет, оценка потенциала, анализ преступности

THE PROBLEMS OF FIGHTING CRIME IN THE HIDDEN DARKNET NETWORK

Abstract:
This article is devoted to the urgent problem of a significant increase in the proportion of crimes committed using information and communication technologies. The main purpose of the study is to improve the methods of analysis and assessment

ISSN: 2835-5733

of crimes committed using information and communication systems and to develop recommendations based on scientific data. The article discusses the main methods and mechanisms for ensuring information security (anonymity on the Internet), as well as promising methods of de-anonymization of users that can be used in the process of detecting and solving crimes. The author proposes a basic crime model designed for the primary study of criminal personalities. A methodology for assessing the potential of information and communication networks is also proposed, taking into account the specifics of using computer tools in criminal activities.

Keywords: Darknet, crime, deanonymization methods, attacker model, crime detection, anonymity, information and telecommunication networks, shadow Internet, potential assessment, crime analysis

Сеть Darknet, известная своей анонимностью и недоступностью для обычных поисковых систем, стала местом, где процветает преступная деятельность. На этой темной стороне интернета происходят сделки с наркотиками, оружием, краденными данными, а также планируются и совершаются другие преступления. Борьба с преступностью в сети Darknet представляет собой серьезное испытание для правоохранительных органов и специалистов по кибербезопасности.

Проблема обеспечения анонимности пользователей в Интернете возникла еще на заре создания и становления публичных коммуникационных сетей. Было бы неверно полагать, что вопросы анонимизации и деанонимизации возникли недавно. Здесь будет уместно напомнить о некоторых технологиях мониторинга (отслеживания) работы пользователей. В основном эти технологии используются в маркетинговых целях и широко востребованы в рекламе (Alexa, SimilarWeb и т. д.)[1]. Однако технологии отслеживания могут успешно применяться и для анонимизации пользователей, и это также является предметом оперативного развития.

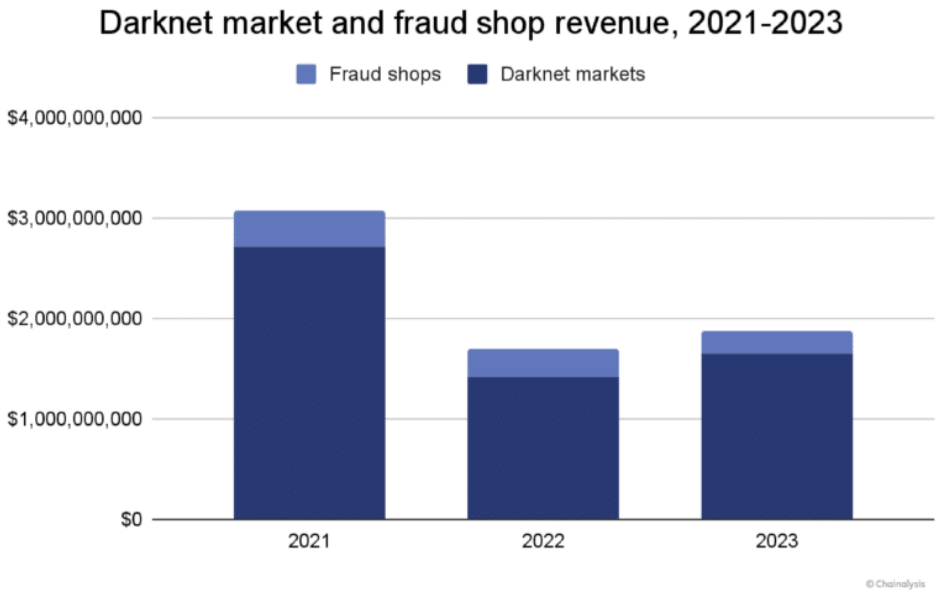
Для начала мы можем рассмотреть типовую схему преступления, в сети отражены различные способы защиты клиентов, например, программа

[1] Гаврилин Ю.В. Использование информации, полученной из сети Интернет, в расследовании преступлений экстремистской направленности/ Ю.В. Гаврилин, А.В. Шмонин. 2021. № 1 (49). С. 105-111.

"Гарант-сервис", которая значительно повышает безопасность денежных операций при использовании электронных денег. Для регистрации электронных денег ("e-money") с использованием наиболее распространенных платежных систем (например, WebMoney, YandexMoney, QIWI) используются три основные технологии: "левая" SIM-карта, готовый "кошелек" и регистрация SIM-карты с "виртуальным номером банковской карты". Несмотря на ужесточение правил, их приобретение и использование обычно не вызывает проблем. Следует отметить, что "анонимные" SIM-карты требуются только на этапе первичной регистрации в ЭПС и в дальнейшем не используются. В дальнейшем злоумышленник открывает счет в ЭПС, обновляет этот счет, открывает "левый" счет в ЭПС, получает криптовалюту, обновляет кошелек и получает криптовалюту. Эта процедура может повторяться несколько раз, пока не будет достигнута главная цель - удлинить цепочку финансовых операций и усложнить процедуру анонимизации для злоумышленника. По аналогичной схеме происходит регистрация "номеров виртуальных банковских карт"; использование ЭПС имеет серьезные недостатки, связанные с ограничением суммы средств. Именно поэтому платежная система QIWI предлагает различные типы кошельков: анонимный, стандартный и максимальный. В случае с анонимными счетами сумма транзакций очень мала, а в случае с максимальными счетами для верификации счета требуется посещение офиса[2]. Очевидно, что такая процедура неприемлема для злоумышленников. Для получения стандартного уровня достаточно предоставить селфи с паспортом в руках и нет необходимости лично посещать офис.

[2] Павличенко Н.В. Сочетание гласных и негласных методов и средств в уголовном процессе: инновация или правовая реальность?/ Н.В. Павличенко, А.И. Тамбовцев. 2017. № 3 (43). С. 111-115.

В следующей диаграмме четко можем увидеть сколько заработали даркнет площадки в разные годы



Суммарная выручка маркетплейсов, работающих в даркнете, за 2023 год достигла $1,7 млрд. Это почти на 25% больше, чем годом ранее, выяснила аналитическая компания Chainalysis.

По данным исследователей, рынок почти оправился от закрытия в 2022 году крупного онлайн-магазина Hydra. И хотя пока ни одна торговая площадка даркнета не может достичь показателей Hydra, доходы восстанавливаются[3].

Данные о росте выручки маркетплейсов в даркнете за 2023 год вызывают серьезные опасения. Увеличение доходов в этой сфере может свидетельствовать о росте преступной деятельности и незаконных операциях. Необходимо принимать меры для борьбы с такими платформами и предотвращения их дальнейшего развития.

Отметим, что даже в открытом интернете существует большое количество ресурсов, предлагающих услуги по предоставлению "фальшивого" фото с паспортом и другими документами. В сети TOR такие сервисы не редкость и легкодоступны. Поэтому наиболее "опасным" этапом для злоумышленников является процедура первичного доступа к ЭПС, в частности, этап покупки SIM-карты: Продажа (покупка) наркотиков ("НС", "ПАВ", "АДД"),

[3] http://hisobot.stat.uz/

психоактивных и сильнодействующих веществ, которые являются одними из самых распространенных преступлений с использованием сети TOR[4]. Рассмотрим пример следующей схемы На торговой площадке обычно размещаются объявления о продаже НС, ПАВ и АДД в двух позициях (предзаказ и готовая казна). Для связи с продавцом используется схема шифрования информации и цифровой подписи файлов (сообщений) на основе GNU Privacy Guard (GPG), в которой всегда используются открытый и закрытый ключи. Открытый ключ обычно прикреплен к профилю пользователя и может быть использован любым человеком; чаще всего используются такие бесплатные программы, как gpg4usb и gpg4win. Получатель создает сообщение, используя открытый ключ "продавца" и свой собственный закрытый ключ, и отправляет его "продавцу". Продавец" проверяет целостность сообщения отправителя и генерирует ответ, используя тот же метод[5]. Покупатель лично или с помощью гаранта приобретает затребованный товар за криптовалюту и получает информацию о местонахождении (закладке) клада. Если используется гарантийный сервис, то гарант переводит криптовалюту "продавцу" после получения и подтверждения клада.

Давайте посмотрим на "темную" сторону закрытого сообщества, которым является темная паутина. К сожалению, использование Anonymous сопровождается незаконной деятельностью.

Первые более-менее доступные сайты темной паутины появились в Узбекистане в 2012 году, когда стала широко доступна стабильно работающая версия браузера Tor. Изначально они были ориентированы на форумы и

[4] Корчагин А.Г. К вопросу о популярности криптовалюты в преступной среде /А.Г. Корчагин, А.А. Яковенко// Гуманитарный журнал. 2020. Т. 9. № 2 (31). С. 390-394.
[5] Гонов Ш.Х., Милованов А.В. Актуальные вопросы противодействия преступности в сети Даркнет // Полицейская и следственная деятельность. 2021. № 1. С. 26-34. DOI: 10.25136/2409-7810.2021.1.34560 URL: https://nbpublish.com/library_read_article.php?id=34560

дискуссионные площадки для общения на специфические или запрещенные темы. Что послужило толчком к криминализации темной паутины? Массовая миграция преступников связана с растущей популярностью криптовалюты Bitcoin и агрессивным пресечением употребления наркотиков со стороны правоохранительных органов.

Вслед за наркодилерами в Темную паутину пришли торговцы оружием, фальшивомонетчики, продавцы поддельных документов и детской порнографии. В результате многие преступники предпочли проводить свои незаконные операции в Интернете.

У правительства нет проблем с анонимайзерами и VPN, расположенными в Узбекистане, но сервисы, находящиеся за пределами России, могут отказаться выполнять предписания российских властей. В то же время от разработчиков Tor не стоит ожидать сотрудничества с государственными органами, поскольку их принцип - анонимность.

Помимо сотрудничества с провайдерами и владельцами сервисов, новый закон также затрагивает поисковые системы и сервисы Google Play и App Store, работающие на территории Узбекистана. Они будут обязаны удалять из результатов поиска ресурсы и программное обеспечение, позволяющее получить доступ к заблокированным ресурсам, в том числе к темной паутине. В случае отказа они также будут заблокированы.

Многие страны мира блокируют интернет-ресурсы в качестве ограничительной меры, но лишь немногие имеют опыт борьбы с подобными мерами. Самый известный пример - опыт Китая в области блокировки, известный как "Великая китайская стена", по аналогии с Великой китайской стеной. Чтобы предотвратить доступ своих граждан к заблокированным сайтам, Китай активно пресекает деятельность служб веб-анонимизации: все новые сервисы, предлагающие VPN-доступ, постоянно блокируются в Китае, что сильно ограничивает возможности Tor. Однако даже серьезные и долгосрочные меры, предпринимаемые Китаем, не дают стопроцентного эффекта, и, несмотря на трудности, жители Китая продолжают пользоваться сервисами анонимности.

Ближайшие соседи Узбекистана также имеют опыт обхода блокировок: в 2015 году аналогичные законы были приняты в Казахстане. В конце 2016 года в

стране начались первые попытки активного внедрения блокировки Tor. К тому времени число пользователей Tor в Казахстане сократилось почти вдвое.

Европейский институт RAND видит следующие основные способы борьбы с преступностью в темной паутине

1. сравнение деятельности в реальном и виртуальном мире. Сравните реальную деятельность, связанную с преступной деятельностью, с деятельностью в Интернете. Например, арест Росса Ульбрихта в 2013 году при использовании публичной сети Wi-Fi совпадает с появлением администраторов Silk Road в виртуальном пространстве.
2. получение данных с публичных сайтов Злоумышленники используют темную паутину только как платформу для совершения своих преступлений, но зачастую они ищут клиентов в общедоступных сетях. По закону владельцы общедоступных сайтов обязаны предоставлять соответствующую информацию полиции. Например, тот же Росс Ульбрихт, который оставил свой адрес электронной почты в общедоступной сети, чтобы связаться с Silk Road.
3. перехват почты. Правоохранительные органы сотрудничают с курьерскими компаниями и почтовыми отделениями для расследования подозрительных посылок. Сотрудники правоохранительных органов также могут записать номер подозрительной посылки и отследить ее получателя.
4. самообучающиеся программные инструменты. Используя большие данные, полицейские могут обнаружить невозможные связи: принимая во внимание IP-адреса и опубликованную в сети информацию, они делают выводы и постепенно обучают искусственный интеллект. Это дорогая и сложная система, но ее использование приносит свои плоды.
5. отслеживание денежных потоков Криптовалюты анонимны, но их слабость заключается в транзакциях. Полиция может запросить у бирж данные о том, кто и когда торговал криптовалютами.
6. Запугивание. Нередко полицейские следователи выдают себя за продавцов, розничных или оптовых торговцев, чтобы войти в доверие к администраторам запрещенных сайтов.
7. хакерство. Правоохранительные органы используют модифицированное программное обеспечение, которое подключается непосредственно к

торговым платформам, форумам или связанным с ними веб-сайтам в темных веб-сетях, создавая уязвимости для перехвата IP-адресов пользователей[6].

Поэтому социальная опасность этого явления очевидна, а эффективность профилактических мероприятий требует повышения. Проанализировав международную борьбу с преступностью в социальных сетях даркнета, можно разработать и успешно внедрить основные методы борьбы с преступностью в даркнете.

Возможность анонимно входить в Интернет и просматривать страницы значительно расширяется благодаря использованию специальных операционных систем, которые не устанавливаются на жесткий диск компьютера. Например, операционная система TAILS - это специальная современная версия Linux Debian; некоторые из программных продуктов, входящих в TAILS: TOR Browser - анонимная веб-программа, Mozilla Thunderbird - приложение для работы с электронной почтой и GNU Privacy Guard - программа для создания зашифрованных сообщений. Mozilla Thunderbird - приложение для работы с электронной почтой, GNU Privacy Guard - программа для создания ключей шифрования и подписи сообщений, KeePassXC - менеджер паролей, Electrum Bitcoin - криптовалютный кошелек, Metadata Anonymisation Toolkit (MAT) - инструмент для анонимизации метаданных. Toolkit (MAT) - программа для удаления метаданных из файлов. Например, программа MAT может использоваться для удаления метаданных из графических файлов. Это связано с тем, что многие современные камеры добавляют к фотографиям метаданные в формате Exif (например, марку и модель камеры, время съемки и т. д.). Хотя в задачи данной работы не входит криминалистическое исследование аппаратного и программного обеспечения, TAILS загружается только один раз, а данные о работе системы хранятся в оперативной памяти и используются только в одном сеансе[7]. Поэтому использование операционной системы TAILS или аналогичных систем свидетельствует о значительном уровне квалификации злоумышленника.

В заключение следует отметить, что проблема преступности в сети Darknet требует комплексного подхода и постоянного совершенствования методов

[6] Taking Stock of the Online Drugs Trade

[7] Новосельцева А.В. Современные методы атак деанонимизации на сеть TOR / А.В. Новосельцева, С.Г. Клюев // Прикаспийский журнал: управление и высокие технологии. 2020. № 1 (49). С. 155-161.

борьбы. Необходимо улучшать сотрудничество между правоохранительными органами различных стран, развивать технологии и методы анализа данных, а также повышать осведомленность общества о рисках, связанных с использованием Darknet. Только совместными усилиями можно добиться прогресса в предотвращении преступной деятельности в этой темной уголке интернета

Более того, методы деанонимизации - это творческий процесс, который не очень эффективен при использовании стандартных методик. Если потенциал злоумышленника высок, деанонимизация становится очень сложной, но выполнимой задачей.

REFERENCES:

1. Гаврилин Ю.В. Использование информации, полученной из сети Интернет, в расследовании преступлений экстремистской направленности/ Ю.В. Гаврилин, А.В. Шмонин. 2021. № 1 (49). С. 105-111.
2. Павличенко Н.В. Сочетание гласных и негласных методов и средств в уголовном процессе: инновация или правовая реальность?/ Н.В. Павличенко, А.И. Тамбовцев. 2017. № 3 (43). С. 111-115.
3. Корчагин А.Г. К вопросу о популярности криптовалюты в преступной среде /А.Г. Корчагин, А.А. Яковенко// Гуманитарный журнал. 2020. Т. 9. № 2 (31). С. 390-394.
4. Гонов Ш.Х., Милованов А.В. Актуальные вопросы противодействия преступности в сети Даркнет // Полицейская и следственная деятельность. 2021. № 1. С. 26-34. DOI: 10.25136/2409-7810.2021.1.34560 URL: https://nbpublish.com/library_read_article.php?id=34560
5. Новосельцева А.В. Современные методы атак деанонимизации на сеть TOR / А.В. Новосельцева, С.Г. Клюев // Прикаспийский журнал: управление и высокие технологии. 2020. № 1 (49). С. 155-161.
6. http://hisobot.stat.uz/
7. Taking Stock of the Online Drugs Trade.
8. URL: https://metrics.torproject.org.