

В. Д. Аверин¹✉

Метод мониторинга работы локальных пользователей электронных вычислительных машин в условиях использования средств анонимизации

¹Национальный исследовательский ядерный университет «МИФИ»,
г. Москва, Российская Федерация
e-mail: vd_averin@mail.ru

Аннотация. В работе рассматривается проблема комплексного мониторинга и контроля действий пользователя в условиях использования им средства анонимизации. Актуальность работы обусловлена ростом целевых атак, в процессе которых используются данные средства. Описываются распространенные вектора атак с точки зрения внутреннего и внешнего нарушителя, которые включают в себя использование данных средств для закрепления, предотвращения обнаружения, получения учетных данных и эксфильтрации. Описывается техническая сложность контроля и непрерывного мониторинга данного типа средств за счет их доступности и распространенности для конечного пользователя. По результатам анализа, предлагается метод, который позволяет по анализу локальных артефактов ЭВМ пользователя определять и реагировать на появление или активацию работы данных средств. Артефакты формализуются и систематизируются на прямые и косвенные признаки, относящиеся к тем или иным типам средств. Предлагается конкретный перечень признаков для операционных систем семейства Windows, а также возможная техническая реализация метода в виде отдельной системы мониторинга, которая может быть интегрирована в работу с другими средствами защиты информации.

Ключевые слова: средства анонимизации, мониторинг пользователей, контроль конечных точек, теневая ИТ

V. D. Averin¹✉

A method for monitoring the activity of local users of electronic computing machines under conditions involving the use of anonymization tools

¹National Research Nuclear University MEPhI (Moscow Engineering Physics Institute),
Moscow, Russian Federation
e-mail: vd_averin@mail.ru

Abstract. The article addresses the problem of comprehensive monitoring and control of user actions under conditions where the user employs anonymization tools. The relevance of the study stems from the increase in targeted attacks that utilize such tools. Common attack vectors from the perspective of both internal and external attackers are described, including the use of these tools for achieving persistence, evading detection, obtaining credentials, and exfiltrating data. The technical complexity of controlling and continuously monitoring this class of tools, arising from their availability and widespread use among end users, is discussed. Based on the analysis, a method is proposed that enables the detection of and response to the appearance or activation of such tools by analyzing local computer artifacts of the user's machine. The artifacts are formalized and categorized into direct and indirect indicators associated with specific types of tools. A concrete set of indicators for Windows

family operating systems is provided, along with a possible technical implementation of the method as an independent monitoring system that can be integrated with other information security systems.

Keywords: anonymization tools, user monitoring, endpoint protection platform, shadow IT

Введение

В условиях стремительного развития и распространения средств анонимизации трафика набирают популярность вектора целевых атак, включающие в свою реализацию использование данных средств, в том числе на этапе закрепления, предотвращения обнаружения, получения учетных данных и эксфильтрации [1]. Злоумышленники целенаправленно комбинируют оверлейные технологии и технологии виртуальных частных сетей для сокрытия своей активности при проведении атаки [2, 3]. Кроме того, перечисленные средства используются не только внешними, но и внутренними нарушителями, например, при инсайдерской деятельности. Согласно [4], доля утечек данных по вине персонала продолжает расти, причём подавляющее большинство инцидентов носят умышленный характер.

К средствам анонимизации в данной работе относят [5]: VPN-клиенты, прокси-сервера, браузерные расширения и оверлейные сети, в частности, сеть Tor. Примерами векторов атак с использованием данных средств могут быть вредоносные VPN-расширения браузеров, осуществляющих перехват конфиденциальных данных пользователей [6], использование модификаций Tor-браузера с незадекларированными возможностями (установления reverse-shell'a и ssh-тоннеля) [7] или использование прокси внутренними нарушителями для минимального воздействия на систему и эффективного обхода сетевой фильтрации [8].

Обуславливается такое внимание к данным средствам с точки зрения атакующих сложностью факта их обнаружения на основе анализа сетевых потоков. Существующие подходы либо ориентированы на постфактум-расследование инцидентов [9], либо требуют специализированной настройки инфраструктуры, например, развертывания собственного прокси-сервера внутри инфраструктуры для глубокого анализа [10]. В следствие чего, такие признаки (переносные версии браузеров и прокси, браузерные расширения и плагины) часто становятся частью «теневого ИТ» – информационных технологий, цифровых устройств, программного обеспечения и ИТ-услуг без одобрения со стороны ИТ- и ИБ-подразделений организации.

Решением данной проблемы может служить строгая политика информационной безопасности, которая запрещает запуск и установку любых исполняемых файлов, а также покупка и переход на корпоративные браузеры, поддерживающие работу с групповыми доменными политиками, например, Яндекс Браузер для Организаций. Однако не всегда такой подход технически реализуем, особенно в СМБ-сегменте в условиях непрерывности бизнес-процессов. Но сам агентный сбор информации, который лежит в основе EPP-решений, позволяет формализовать метод обнаружения прямых и косвенных признаков наличия средств анонимизации на конечных точках.

Целью данной работы является разработка и формализация метода мониторинга активности пользователя, который систематизирует и выявляет прямые и косвенные признаки использования средств анонимизации (VPN-клиентов, прокси-серверов, браузерных расширений и Tor Browser) на основе анализа локальных артефактов операционной системы. Целевой операционной системой являются ОС семейства Windows, однако предлагаемый метод расширяется и до Unix-подобных систем, для которых будет необходимо переопределение способов реализации получения признаков.

Предлагаемый метод мониторинга

В основе метода лежит процесс инициализации цифрового профиля пользователя, который работает за определенным АРМ. Профиль включает в себя параметры операционной системы, перечень которых будет представлен далее. Ниже представлена блок-схема предлагаемого метода (рис. 1).

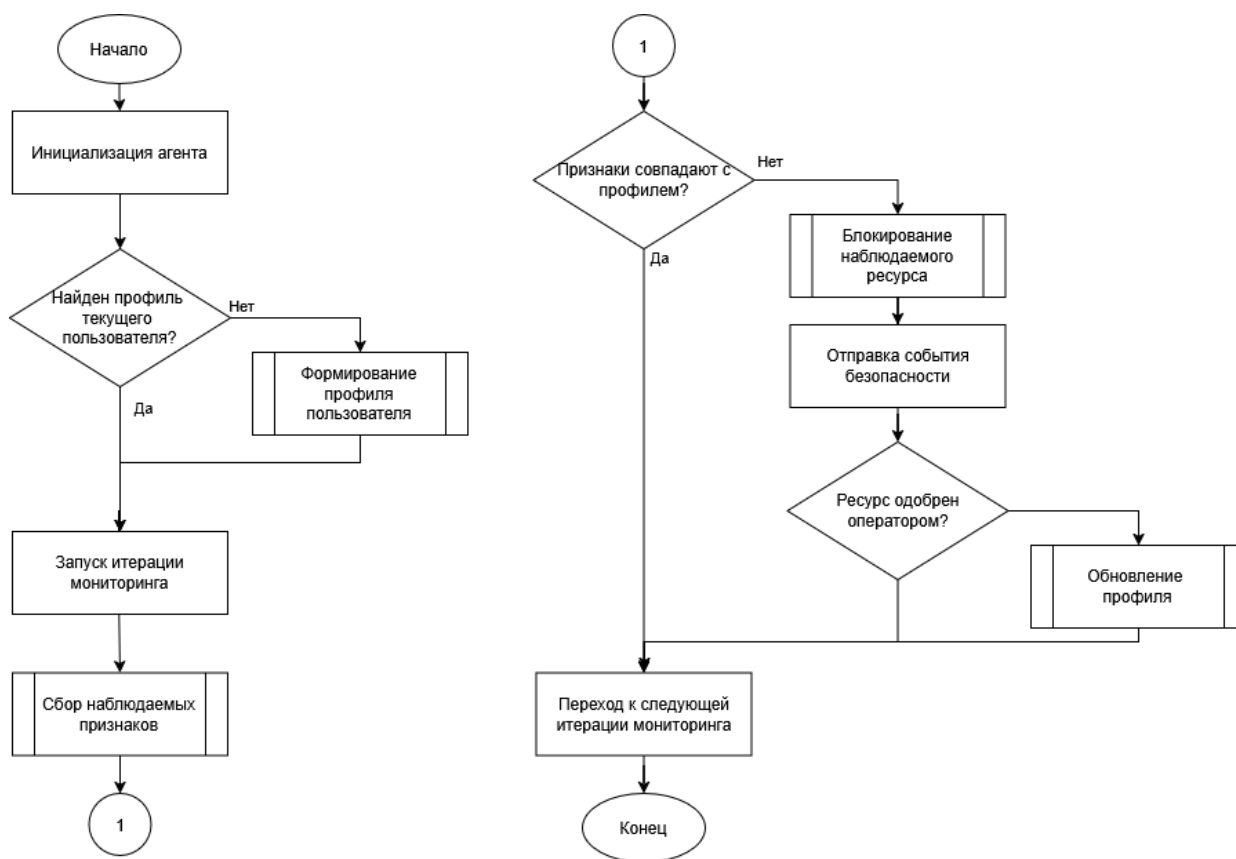


Рис. 1. Блок-схема предлагаемого метода

Как было сказано ранее, под наблюдаемыми средствами анонимизации в работе рассматривается следующий перечень: VPN-клиенты типа Remote Access, прокси-клиенты, расширения и плагины браузеров, и наличие на АРМ Tor-based браузеров. После формирования профиля включается процесс непрерывного мониторинга параметров и сравнение их изменений с текущим профилем. Так как условия работы и трудовые обязанности сотрудников меняются достаточно редко,

сформированный профиль будет достаточно четко описывать их рабочее окружение. В зависимости от характера изменений метод предусматривает внесение корректировок либо в сам профиль, либо формирование события безопасности, которое передается в службу по реагированию на инциденты.

Необходимо выделить признаки, которые предлагается рассматривать в рамках разрабатываемого метода.

VPN-клиенты удаленного доступа. В случае программной реализации средства его обязательной частью является создание и последующее включение виртуального сетевого интерфейса типа TUN или TAP, а также внесение изменения в таблицу маршрутизации [11]. Наличие данного типа изменений в совокупности указывает на создание нового соединения, но не является прямым признаком использования конкретно VPN-клиента. Например, виртуальные интерфейсы и маршруты также создаются при использовании гипервизоров (может быть необходимо отделу разработки/DevOps) или при подключении периферийных устройств, не имеющих возможности работы по протоколу IP (старые принтеры, телефония, камеры). В этом случае интерфейс будет физическим. Поэтому при начальной инициализации перечня разрешенных интерфейсов и их настроек необходим ручной анализ параметров. Кроме того, для внесения изменений в сетевые настройки системы процессу необходимы административные права. Поэтому несанкционированные изменения такого рода уже становятся прямым признаком компрометации административной учетной записи.

Прокси-клиенты. В отличие от VPN-тоннелей, виртуализирующих новый сетевой интерфейс, прокси-серверы не требуют для своей работы административных прав, так как работают на прикладном уровне. Однако прокси также используется в некоторых аналогах VPN-клиентов, которые технически просто выступают средством настройки для передачи трафика до прокси-сервера VPN-сервиса. Поэтому наличие в системе данных параметров также является наблюдаемым признаком. Примером легитимного использования прокси-клиентов может являться система Банк+Клиент СФТ, в составе которой есть подсистема InterPRO Client. Компонент для обеспечения работы TLS/SSL вместе с российскими криптографическими примитивами включает локальный прокси на стандартном адресе 127.0.0.1:2080. Поэтому данный признак также требует анализа со стороны оператора системы.

Расширения браузеров. Для поиска установленных браузеров и их расширений предлагается анализировать файлы в поиске соответствующих директорий, где хранятся установленные расширения, в том числе их метаданные и состояния (включено/выключено). Например, для Chromium-браузеров такой путь по умолчанию: «%LOCALAPPDATA%\Google\Chrome\User Data\Default\Secure Preferences». Однако нужно понимать, что браузер возможно установить в другое расположение или использовать переносные версии. Поэтому поиск и анализ должен происходить непосредственно по маске внутренних директорий. Для Chromium это «Chrome\User Data\Default\Secure Preferences». Данные расположения и парсинг расширений реализуется на программном уровне. Также нужно учитывать, что у одного пользователя может быть одновременно несколько экземпляров браузеров и профилей в них.

Браузер Tor. Большинство работ по анализу активности Tor полагаются на сетевые методы обнаружения [12-14]. Более того, браузер целенаправленно разрабатывался для сокрытия своей деятельности в системе, поэтому даже запускаемый браузером процесс имеет название «firefox.exe», так как является технически его форком. Однако если обратиться к опыту форензики, можно заметить несколько основных компонент браузера, которые участвуют в его работе постоянно и внедрены в его код статически: это файл torrc, который управляет поведением Tor и хранит полный путь до рабочей директории браузера, а также реализации мостов (транспорты), которые используются для обхода ограничений работы Tor на сетевом уровне [15]. Эти транспорты хранятся в директории PluggableTransports и должны иметь строго определенные имена: snowflake.exe, conjure-client.exe и lyrebird.exe. Наличие хотя бы одного из данных артефактов указывает на наличие данного браузера на хосте.

Таблица 1. Таблица соответствия типов средств с их признаками, техники их обнаружения и блокирования

Тип средства	Признаки	Техника обнаружения
VPN-клиент	Появление TUN/TAP интерфейсов; изменение таблицы маршрутизации	Реестр: HKEY_LOCAL_MACHINE\SYSTEM\CurrentControlSet\Services\Tcpip\Parameters\Interfaces\ Поиск событий журнала Windows Network-Profile/Operational: ID 4001, 4002, 4004, 10001
Прокси-клиент	Появление системных прокси	Powershell: Netsh winhttp show proxy
Расширения браузеров	Появление новых браузеров и переносных версий; появление новых расширений	Поиск директорий браузеров и их парсинг; Chrome: ~.\Chrome\User Data\[Имя_профиля]\Extensions\ Яндекс Браузер: ~.\Yandex\YandexBrowser\User Data\[Имя_профиля]\Extensions\
Использование Tor	Появление файлов конфигурации; появление	Поиск файла torrc и его парсинг. Наличие любого процесса из PluggableTransports: conjure-client.exe, lyrebird.exe, snowflake.exe и др.

В результате процесс инициализации профиля пользователя состоит в анализе инженером информационной безопасности полученных данных и фильтрации разрешенных параметров хоста – сетевого интерфейса, локальных прокси, а также списка разрешенных браузеров и их расширений. При дальнейшем нарушении установленного профиля ресурс, вызвавший изменение профиля, блокируется, а событие безопасности отправляется на сервер для последующего одобрения либо подтверждения блокирования.

Блокирование ресурсов предлагается реализовывать системными утилитами, в зависимости от типа обнаруженного признака. Для сетевых интерфейсов и прокси-соединений это отключение не одобренного интерфейса и настроек прокси, для браузеров удаление/отключение не одобренного расширения и перезапуск браузера, для Tor – заморозка процессов, которые обращаются к данному файлу (реализуется, например, подключением журналирования Sysmon).

Типы средств, относящиеся к ним наблюдаемые признаки и технические варианты их обнаружения применительно к Windows представлены в табл. 1.

Результаты

Экспериментальное исследование предложенного метода реализовано в виде отдельного программного модуля с клиент-серверной архитектурой на стеке C# (агенты) + Kotlin/JavaScript/MariaDB (сервер). На сервере происходит создание исполняемых файлов агентов для распределения по клиентским машинам со своими уникальными идентификаторами. Агенты устанавливаются на хосты как системные службы (от имени SYSTEM, что можно централизованно реализовать, например, через сервер Kaspersky Security Center). Агенты присылают все собранные метрики на сервер только на этапе инициализации для создания профиля для данного агента; дальнейший процесс сравнения с профилем реализуется через логику агента, который отправляет события безопасности серверу только при его изменении либо несоответствии.

Итоговые нагрузочное и интеграционное тестирования разработанного решения проводились в рамках реальной инфраструктуры, состоящей из 46 конечных устройств с установленными агентами. На этапе формирования цифровых профилей было установлено 35 несогласованных с ИТ- и ИБ-отделами ресурсов, среди которых были: 21 расширение браузеров, 6 признаков наличия переносных версий несогласованных браузеров (в основном Opera Browser за счет встроенного в него VPN), 4 прокси-клиента, 3 признака наличия Tor-браузера (2 из которых подтвердили действительную портативную версию у сотрудника на корпоративном съемном носителе) и 1 VPN-клиент. Одобренные ресурсы насчитывали 21 уникальную запись, среди которых самыми распространенными являлись КристоПро ЭЦП Browser plug-in (расширение), 1С Предприятие 8 (прокси-клиент), ГПБ СФТ (прокси-клиент) и Диаг.Плагин.

Обсуждение

Разработанный метод позволяет реализовать непрерывный мониторинг сегмента теневой ИТ, которая чаще всего используется внутренними и внешними нарушителями, при этом не прибегая к ужесточению политики информационной безопасности, которая для малого и среднего бизнеса может быть неприменима. В отличие от существующих DLP-систем, где наблюдаемые метрики могли выступать в лучшем случае в роли признаков в признаковом пространстве, а значит не несли в себе конкретного указания на активность пользователя, данный метод приравнивает изменения этих метрик к событиям безопасности. Это позволяет провести интеграцию с SIEM-решениями системы, разработанной на основе предлагаемого метода.

Для этого необходимо реализовать коннекторы и правила корреляции, которые смогут обогащать контекст с учетом производимых пользователем действий.

Кроме того, полученный перечень одобренных ресурсов в рамках тестирования позволяет реализовать автоматизированное создание новых профилей пользователей, что значительно упрощает дальнейшую работу и поддержку системы.

Заключение

По результатам работы был предложен метод мониторинга работы локальных пользователей электронных вычислительных машин в условиях использования средств анонимизации, а также перечень наблюдаемых признаков для каждого из типов средств применительно к операционным системам семейства Windows.

Предложенный метод был реализован программно и протестирован в условиях непрерывности бизнес-процессов на существующей инфраструктуре, что позволило получить численные метрики системы, а также сформировать перечень одобренных наблюдаемых ресурсов. Дальнейшая работа может заключаться в модификации метода для автоматизированного реагирования на события безопасности и интеграции разрабатываемой системы с существующими решениями по информационной безопасности класса DLP, SIEM и EPP.

БИБЛИОГРАФИЧЕСКИЙ СПИСОК

1. Усманов А. Р. Методы обнаружения фишинга на основе анализа поведения пользователя // Вестник науки. – 2025. – №6 (87). – С. 710–721.
2. Басыня Е. А., Хиценко В. Е., Рудковский А. А. Метод идентификации киберпреступников, использующих инструменты сетевого анализа информационных систем с применением технологий анонимизации // Доклады ТУСУР. – 2019. – Т. 22. – №2. – С. 45–51.
3. Гайдин А. И., Головчанский А. В. Средства анонимизации в механизме преступной деятельности, осуществляемой в сети Интернет // Вестник Воронежского института МВД России. – 2022. – №2. – С. 205–213.
4. InfoWatch. Утечки данных вследствие действий внутренних нарушителей. Мир – Россия 2022–2025 гг. [Электронный ресурс]. – URL: <https://www.infowatch.ru/sites/default/files/analytics/files/utechki-dannykh-vsledstviye-deystviy-vnutrennikh-narushiteley.pdf> (Дата обращения: 22.04.2026).
5. Нефедов В. С. Кriuлин А. А., Потерпеев Г. Ю. Основы обеспечения анонимности в сети Интернет : учеб. пособие. – Москва: РТУ МИРЭА, 2022. – 81 с.
6. VPN-расширение для Chrome перехватывает запросы пользователей к ИИ [Электронный ресурс] // Xaker.ru. – URL: <https://xaker.ru/2025/12/17/ai-urban-vpn/> (Дата обращения: 22.04.2026).
7. Security Week 2241: браузер Tor с бэкдором [Электронный ресурс] // SecurityLab.ru : блог компании Kaspersky. – URL: <https://www.securitylab.ru/blog/company/kaspersky/352390.php> (дата обращения: 22.04.2026).
8. Чужое в допустимом контуре [Электронный ресурс] // itsec.ru. – URL: <https://www.itsec.ru/articles/chuzhoe-v-dopustimom-konture> (дата обращения: 22.04.2026).
9. Гончар В. В., Аветисян Б. Р. Актуальные направления деанонимизации правонарушителей в сфере ИТ // Вестник экономической безопасности. – 2024. – №1. – С. 61–66.

10. Канатьев К.Н., Гребенщиков А. А. Каравцев Н. А. Передовые методы обнаружения и обфускации VPN-трафика: углубленный анализ OpenVPN и его уязвимостей в современную цифровую эпоху // Инновации и инвестиции. – 2023. – №10. – С. 211–215.
11. Чубахиро А., Каманде М. В. Виртуальные вычислительные сети для случая аппаратной виртуализации // Современная наука: актуальные проблемы теории и практики. Серия: Естественные и Технические Науки. – 2020. – № 6. – С. 158–163.
12. Manjesh P Shetty Dark & deep Web: advanced forensic analysis of Tor Browser and implications for law enforcement agencies // Centre For Cybercrime Investigation Training & Research. – 2022. – 67 с.
13. Amir Aboubakr Shaker Mahmoud, Animesh Kumar Agrawal, Nilay R. Mistry DarkExtract: tool for extracting and analysing Tor Browser host-based activities // International Journal of Electronic Security and Digital Forensics. – 2025. – Vol. 17. – №5. – С. 563–581.
14. Matt Muir, Petra Leimich, William J Buchanan A Forensic Audit of the Tor Browser Bundle // Digital Investigation. – 2019. – Vol. 29. – С. 118–128.
15. Вехов В. Б., Смушкин А. Б. Криминалистическое исследование цифровых отпечатков компьютерных устройств // Всероссийский криминологический журнал. – 2024. – Т. 18. – №4. – С. 390–397.

© В. Д. Аверин, 2026