АКАДЕМИЯ МВД РЕСПУБЛИКИ БЕЛАРУСЬ

Кафедра информационного права
факультета криминальной милиции

Применение технологий искусственного интеллекта для формирования цифрового профиля лица, совершающего преступления с использованием вредоносных компьютерных программ

В.И. Пикта
старший преподаватель кафедры информационного права
Доклад на научной конференции

Минск · 2026

Генеративный ИИ снижает порог входа в компьютерную преступность

10–15 лет назад

Для создания ВКП нужны познания в программировании, сетях и защите информации. Круг лиц узок, подготовка служит ориентиром

Генеративные модели

«Вайб-кодинг»: рабочий код по текстовому описанию. Можно создать ВКП, адаптировать чужой код, автоматизировать атаку

Сегодня

Круг лиц расширяется, личность «хакера» меняется. Прежние ориентиры идентификации работают хуже

≈ 37 %

доля киберпреступлений в общей преступности Беларуси, 2026 г.

≈ 6 %

снижение числа киберпреступлений к 2025 г. — впервые за последние годы

Вывод: нужна методика идентификации, не опирающаяся на профессиональный портрет «хакера»

Источники: статистические данные МВД Республики Беларусь(01.09.2026).

01

ВОПРОС 1

Цифровой профиль: понятие и структура

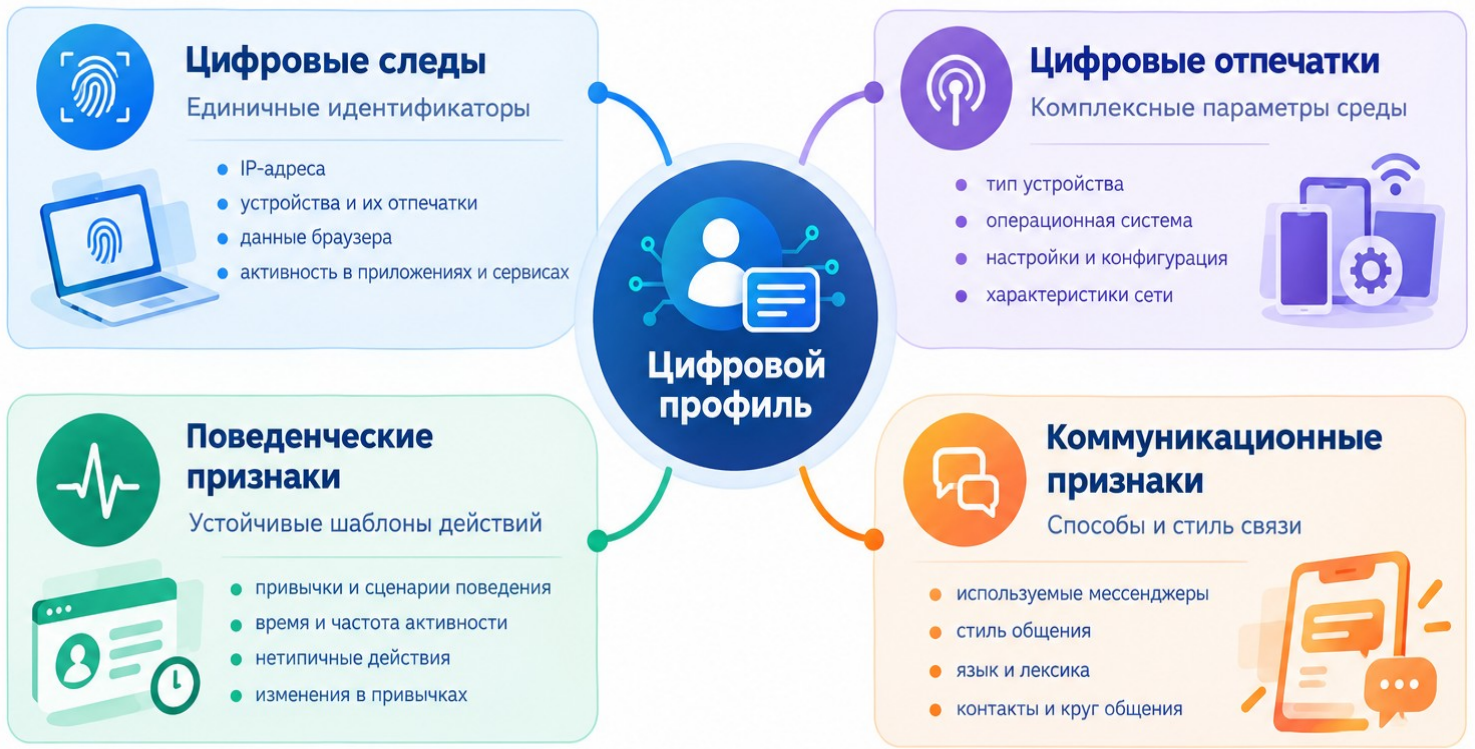
- Понятие цифрового профиля
- Цифровой след и цифровой отпечаток
- Барьеры формирования профиля

Цифровой профиль: понятие и четыре элемента

ОПРЕДЕЛЕНИЕ

Цифровой профиль — структурированная совокупность технических, лингвистических и поведенческих признаков, извлечённых из цифровых следов преступной деятельности и позволяющих сузить круг причастных лиц либо связать отдельные эпизоды

Анонимизация нейтрализует любой элемент по отдельности, **но не всю их совокупность**



Цифровой след и цифровой отпечаток — не синонимы

Критерий	Цифровой след	Цифровой отпечаток
Природа	Единичный идентификатор	Комплексный идентификатор
Как возникает	В результате конкретного действия злоумышленника	Из совокупности технических параметров устройства или программной среды
Примеры	IP-адрес, доменное имя, идентификатор учётной записи	Конфигурация программного и аппаратного обеспечения, параметры среды ВКП
Устойчивость	Нейтрализуется VPN, TOR, NAT	Сохраняется при анонимизации в пределах определённого периода

Три барьера формирования цифрового профиля

1

Реверс-инжиниринг

Сведения нужно извлечь из тела ВКП, а это требует знания машинного кода и специальной подготовки

2

Анонимизация

VPN, TOR, NAT и иные средства нейтрализуют отдельные цифровые следы злоумышленника

3

Разнородность данных

Технические, лингвистические и поведенческие данные традиционно анализируют разные специалисты

Задача ИИ — снять каждый барьер: автоматизировать анализ кода, опереться на устойчивые признаки, объединить разнородные данные

02

ВОПРОС 2

Направления применения искусственного интеллекта

- Анализ кода агентными ИИ-системами
- Стилометрия и обработка естественного языка
- Поведенческие и организационные признаки

Агентные ИИ-системы делают код ВКП читаемым

Образец ВКП

Исполняемый файл, машинный код

Вызов инструментов

Агент сам запускает дизассемблер через командную строку

Восстановление смысла

Имена функций и переменных, комментарии к коду

Извлечение «секретов»

Адреса C2-серверов, ключи шифрования, учётные данные

Скорость

Анализ быстрее ручного реверс-инжиниринга: аналитик не участвует в каждой операции

Доступность

Снижается порог входа для сотрудников, противодействующих преступлениям с ВКП

Авторство кода и лингвистический портрет

2 Стилометрия кода

ПРИЗНАКИ

структура синтаксических деревьев, предпочитаемые конструкции, обработка ошибок

МЕТОД

статический анализ или ИИ-агент ⟶ классификатор машинного обучения

РЕЗУЛЬТАТ

связь образцов ВКП по разным уголовным делам с одним лицом или группой

Caliskan-Islam A. et al., 2015

3 Обработка естественного языка

ДАННЫЕ

переписка на теневых форумах, комментарии в коде, метаданные инфраструктуры

МЕТОД

ИИ-агент собирает материалы, NLP-модели выявляют лексические и синтаксические маркеры

РЕЗУЛЬТАТ

лингвистический портрет, связь публикаций под разными учётными записями

Поведенческие и организационные признаки

Время активности

часовой пояс, режим работы злоумышленника

Обращения к C2

временные шаблоны связи ВКП с серверами управления

Инфраструктура

повторное использование сетевых ресурсов

Монетизация

устойчивые схемы извлечения дохода

Заражение → требование

типичный интервал между этапами

Переговоры с жертвой

характерная тактика ведения

Анализ журналов: ИИ-агенты сами выдвигают и проверяют гипотезы. Методологическая основа — поисковый портрет серийного преступника (Бессонов А. А., 2021)

Какой барьер снимает каждое направление

Направление	Инструмент ИИ	Основной барьер	Элемент профиля
1 · Анализ кода	Агентные системы + дизассемблеры	Реверс-инжиниринг	Технические признаки, «секреты», инфраструктура
2 · Стилометрия	Машинное обучение, агентный анализ кода	Анонимизация	Цифровой отпечаток автора кода
3 · Язык	Агентный сбор + NLP-модели	Анонимизация	Коммуникационные признаки
4 · Поведение	Агентный анализ сетевых журналов	Разнородность данных	Поведенческие признаки

Идентификационную ценность даёт не отдельное направление, а их совокупность — интегральный профиль

03

ВОПРОС 3

Реализация и ограничения

- Сопоставление с оперативно-розыскными сведениями
- Правовой статус выводов ИИ
- Ограничения и авторская позиция

Сопоставление профиля со сведениями ОРД

1 **Технический профиль**
результаты четырёх направлений анализа

2 **Систематизация**
ИИ-агент сводит индикаторы компрометации

3 **Сопоставление**
со сведениями, полученными в порядке Закона об ОРД

4 **Ориентирующая информация**
определяет направления конкретных ОРМ

ПРАВОВОЙ СТАТУС ВЫВОДОВ ИИ

Не доказательство, а ориентирующая информация

Автоматизированные выводы определяют направления оперативно-розыскных мероприятий и требуют проверки установленными законом средствами

Закон Респ. Беларусь от 15 июля 2015 г. № 307-З «Об оперативно-розыскной деятельности»

Ограничения применения ИИ и авторская позиция

«Чёрный ящик»

непрозрачность моделей затрудняет проверку выводов

Вероятностный характер

нужна экспертная верификация по апробированной методологии

Противодействие

виртуальные машины, антидетект-браузеры, шифрование каналов

ИИ — вспомогательный инструмент, а не средство доказывания

Дополняет, но не подменяет традиционные методы противодействия преступлениям с ВКП. Надёжный вывод требует нескольких независимых элементов профиля, а не отдельного цифрового следа

Выводы

I

Генеративный ИИ снижает порог входа в компьютерную преступность и расширяет круг лиц, использующих ВКП, — подходы к идентификации требуют пересмотра

II

Цифровой профиль как совокупность следов, отпечатков, поведенческих и коммуникационных признаков устойчив к анонимизации; ИИ снимает барьеры его формирования

III

Выводы ИИ носят ориентирующий характер и требуют сочетания с оперативно-розыскными и криминалистическими методами

Благодарю за внимание

ГОТОВ ОТВЕТИТЬ НА ВОПРОСЫ

В.И. Пикта
кафедра информационного права
Академия МВД Республики Беларусь