

Т. И. Мишуткина

Цифровой след как элемент национальной безопасности

В контексте растущей цифровизации общества осмысливаются феномен «цифровой след» (digital footprint) и его влияние на национальную безопасность Республики Беларусь. Рассматриваются такие его аспекты, как электронный, виртуальный и информационный. Анализируется использование цифрового следа во всех сферах жизни общества, в том числе в правоохранительной деятельности. Эффективным инструментом для формирования у будущих офицеров осознанного отношения к последствиям их онлайн-действий является социокультурное проектирование, направленное на развитие необходимых компетенций. Подчеркивается, что понятие «цифровой след», представляющее многослойное и комплексное явление, совершенствуется вместе с новейшими технологиями и требует внимательного изучения и сознательного подхода к управлению собственной онлайн-активностью.

Ключевые слова: цифровой след, электронный след, виртуальный след, информационный след, социокультурное проектирование, национальная безопасность, цифровая культура, цифровизация, онлайн-активность.

T. Mishutkina

Digital footprint as an element of national security

In the context of the growing digitalization of society, this article examines the phenomenon of the "digital footprint" and its impact on the national security of the Republic of Belarus. The author examines its electronic, virtual, and informational aspects, analyzing the use of the digital footprint in all spheres of society, including law enforcement. Sociocultural design aimed at developing the necessary competencies is an effective tool for developing future officers' conscious attitude toward the consequences of their online actions. The concept of "digital footprint" is a multilayered and complex phenomenon, which is evolving alongside the latest technologies and requires careful study and a conscious approach to managing one's online activity.

Keywords: digital footprint, electronic footprint, virtual footprint, informational footprint, sociocultural design, national security, digital culture, digitalization, online activity.

Современные условия жизни отличаются ростом образовательного уровня населения, а также изменениями в социальной структуре общества. Развитие глобальной сети Интернет, социальных медиа и цифровизация способствуют переносу части общественных взаимодействий в цифровую сферу, что приводит к возникновению новых форм сотрудничества между государством и гражданами. Увеличение информационной открытости способствует повышению доверия населения, которое разделяет с государством ответственность за будущее страны [4].

В современной действительности вопрос цифровизации общества стал одним из важнейших и наиболее дискутируемых. Тема цифрового следа в сфере национальной безопасности находится в процессе становления. Ряд ученых, среди которых С. Р. Низаева, Е. Р. Россинская и И. А. Рядовский, А. Н. Ундозерова, А. А. Эльтемеров и О. В. Эльтемерова активно работают над понятием «цифровой след» и определяют его как совокупность данных и информации, которые пользователи оставляют в процессе взаимодействия с цифровыми устройствами, интернет-ресурсами и онлайн-сервисами [3; 5; 7; 8]. Однако стоит отметить, что опыт вышеперечисленных авторов следует применять, учитывая специфику и особенности нашей страны.

Цель статьи – обоснование феномена «цифровой след» в контексте национальной безопасности.

Стремительный рост цифровизации общества приводит к значительному увеличению онлайн-активности во всех сферах жизни общества, что представляет собой актуальную научную проблему. Принципиальное значение цифровой след занимает в системе национальной безопасности Республики Беларусь. Важно понимать, что вопросы виртуальной реальности надо рассматривать не просто с технической стороны, а следует учитывать этические и правовые проблемы. Формирование у курсантов компетенций безопасного и эффективного использования онлайн-пространства становится неотъемлемой частью подготовки будущих офицеров, а грамотное использование виртуальной среды способствует укреплению национальной безопасности.

Сегодня Республика Беларусь активно поддерживает развитие и популяризацию цифрового контента, для этого государство внедряет современные технологии во все сферы жизни. По уровню «информатизации» Республика Беларусь входит в число стран с высоким и выше среднего значением ее развития, при этом информационное пространство страны остается открытым и высококонкурентным» [1, с. 10]. Удельный вес населения Республики Беларусь, использующего Интернет, постоянно растет: в 2022 г. он составил 89,5 %, в 2023 г. – 91,5 %, а в 2024 г. достиг 94,3 % [6]. Это подтверждает тенденцию к увеличению охвата населения сетью.

Пропорционально увеличивается и количество времени, проведенное ежедневно в Интернете, и количество проводящих операций соответственно. Просмотр сайтов, совершение онлайн-покупок, оплата услуг, пользование социальными сетями, обмен информацией, данными и фотографиями, использование фитнес-трекеров, подключенных к Интернету, – все эти действия оставляют цифровой след. Расцвет цифровых технологий пришелся на время пандемии коронавируса, появилось огромное количество сервисов, образовательных ресурсов и других средств коммуникаций, которые перешли в онлайн-режим. Период

карантина прошел, а виртуальный функционал плотно внедрился в реальную жизнь.

Понятие «цифровой след» обозначает совокупность действий, оставленных пользователем в цифровой среде. Термин стали использовать в начале 2000-х гг. для определения взаимосвязи между онлайн-активностью и ее последствиями в реальном мире [3; 7; 8].

Ранее применялись более узкие определения, такие как «электронный след», «виртуальный след», «информационный след», каждый из этих терминов акцентирует внимание на определенном аспекте этого феномена. «Электронный след» ориентирован на физическую составляющую – это конкретные файлы, данные, сигналы, передаваемые по электронным каналам связи.

«Виртуальный след» подчеркивает нематериальную природу отпечатка – это виртуальные объекты, интерактивные элементы, сообщения в социальных сетях, комментарии на форумах, виртуальные покупки, онлайн-игры и достижения в них. «Виртуальный след» описывает абстрактную сторону процесса, фокусируясь на отсутствии физической формы, но сохраняя реальность воздействия.

«Информационный след» сосредоточивается на содержании оставляемой информации – это сама суть данных, их семантика и контекст, может включать личные данные, профессиональную информацию, предпочтения, мнения и убеждения. Понятие «цифровой след» объединяет все эти аспекты и подчеркивает важность понимания осознанности онлайн-активности.

С. Р. Низаева, А. Н. Ундозерова и другие ученые выделяют два основных вида цифровых следов: пассивный и активный. Пассивный след «представляет собой информацию, собранную о пользователе без его ведома; в ряде случаев эти данные непреднамеренно оставляет сам пользователь» [3, с. 189]. Например, персональные данные (имя, возраст, пол); поведенческие данные (история поиска, просмотренные страницы); финансовые данные (история покупок, информация о банковских картах); геолокационные сведения (местоположение, IP-адрес); технические данные (тип устройства, операционная система). Активный след состоит из сведений, которые пользователь публикует в Интернете по собственной инициативе (регистрация в соцсетях, заявки на участие в конкурсах, заполненные формы и анкеты, обмен сообщениями в режиме реального времени или на форумах и в чатах) [7].

Цифровой след используется как для законных целей, например для персонализированной рекламы, профилирования пользователей, анализа потребительского поведения, так и для злонамеренных – мошенники с помощью цифровых данных создают целевые атаки, например фишинговые письма, чтобы украсть личную информацию; несанкционированный доступ к вашей информации также является противо-

правным действием. Более того, современные технологии (например искусственный интеллект) позволяют анализировать цифровые следы достаточно качественно, что приводит к появлению новых этических и правовых вопросов, связанных с защитой личных данных.

Важно отметить, что чаще всего в своей практике понятием «цифровой след» пользуются сотрудники внутренних дел. На взгляд Е. Р. Россинской и И. А. Рядовского, «цифровой след представляет собой криминалистически значимую компьютерную информацию о событиях или действиях, отраженную в материальной среде, в процессе ее возникновения, обработки, хранения и передачи» [5, с. 7]. В МВД разработана и эффективно используется автоматизированная информационная система «Цифровой след», которая обеспечивает накопление, систематизацию и анализ всех цифровых следов, зафиксированных в ходе рассмотрения обращений граждан и дальнейшего расследования уголовных дел [2].

В контексте служебной деятельности цифровой след становится фактором национальной безопасности. Курсанты военных кафедр, будущие офицеры, представляют собой особую категорию, готовящуюся к работе в условиях повышенной ответственности и секретности. Неосторожное обращение с информацией в цифровом пространстве может привести к серьезным последствиям, поэтому формирование осознанного отношения к цифровому следу у курсантов является необходимым условием обеспечения безопасности государства. Важно отметить, что курсанты военной кафедры пользуются Интернетом в свободное время. Молодые люди играют в онлайн-игры, просматривают развлекательный контент на видеоплатформах и общаются в социальных сетях, не анализируя информацию и не учитывая последствий своих действий. Демонстрируемое онлайн-поведение влияет на репутацию, доверие со стороны командования и общества. Неосмотрительные публикации, регистрации, фотографии, комментарии могут стать мощным инструментом пропаганды и дискредитации. Следует помнить, что даже удаленные данные, благодаря современным технологиям восстановления информации, могут быть извлечены и использованы. Курсантам военных кафедр, как и всем военнослужащим, следует осознанно подходить к поведению в Интернете, учитывать последствия своих действий и развивать навыки анализа информации.

Несмотря на то, что мы постоянно оставляем в цифровой сфере множество следов своей онлайн-активности, четкое определение понятия «цифровой след» находится на стадии формирования. Вместе с тем можно сказать, что «цифровой след» – это комплексное определение, охватывающее полный спектр информации, оставляется человеком в Интернете и других цифровых средах, включая активные действия (посты, лайки) и пассивные (IP-адрес, история посещений). Это мно-

гослойная дорожка, обширное множество информации, генерируемое каждый день при использовании различных цифровых сервисов, приложений и устройств. В него входят все типы сведений от истории поиска до данных о местоположении, финансовых транзакциях и прочих взаимодействиях в виртуальном пространстве. Поскольку способы применения цифровых технологий постоянно развиваются, понятие «цифровой след» также продолжает конкретизироваться. Формирование осознанного отношения к цифровому следу является стратегической задачей, обеспечивающей национальную безопасность. В этой связи социокультурное проектирование представляет собой эффективный инструмент решения данной задачи, позволяющий сформировать у будущих офицеров необходимые навыки и компетенции для безопасного и ответственного использования цифровых технологий.

Проведенное исследование позволяет констатировать, что феномен цифрового следа из сугубо технического или криминалистического понятия трансформировался в многоаспектное явление, оказывающее непосредственное влияние на национальную безопасность. В условиях цифровой трансформации белорусского общества, характеризующейся рекордным проникновением Интернета, вопросы осознанного управления цифровым следом переходят из разряда частных в разряд стратегических государственных задач.

Таким образом, формирование осознанного и ответственного отношения к цифровому следу у будущих офицеров является не просто элементом учебной программы, а стратегическим императивом, напрямую влияющим на суверенитет и национальную безопасность Республики Беларусь. Дальнейшие исследования в данном направлении видятся в разработке конкретных педагогических методик, учебно-методических комплексов и критериев оценки уровня сформированности цифровой компетентности у военных специалистов, что станет практическим вкладом в укрепление обороноспособности страны в цифровую эпоху.

1. Концепция национальной безопасности Республики Беларусь : решение Всебелорус. нар. собр. от 25 апр. 2024 г. № 5. – Минск : Нац. центр правовой информ. Респ. Беларусь, 2024. – 62 с. – (Правовая библиотека НЦПИ).

2. Кубраков представит опыт работы МВД по противодействию киберпреступности коллегам из стран СНГ // БЕЛТА. Новости. – URL: <https://belta.by/society/view/kubrakov-predstavit-opyt-raboty-mvd-po-protivodejstvu-kiberprestupnosti-kollegam-iz-stran-sng-588181-2023/> (дата обращения: 10.07.2025).

3. Низаева, С. Р. Цифровые следы. Виды, перспективы использования в целях раскрытия и расследования преступлений / С. Р. Низаева // Государственная служба и кадры. – 2020. – № 4. – С. 189–190.

4. О реализации основ идеологии белорусского государства : директива Президента Респ. Беларусь, 9 апр. 2025 г. № 12 // Национальный правовой Интернет-портал Республики Беларусь. – URL: <https://pravo.by/document/?guid=12551&p0=P02500012> (дата обращения: 10.07.2025).

5. *Россинская, Е. Р.* Концепция цифровых следов в криминалистике / Е. Р. Россинская, И. А. Рядовский // Аубакировские чтения : материалы Междунар. науч.-практ. конф., Алматы, 19 февр. 2019 г. / Алматинская акад. МВД Казахстана. – Алматы, 2019. – С. 6–8.

6. Статистика информационно-коммуникационных технологий // Национальный статистический комитет Республики Беларусь. – URL: ([дhttps://dataportal.belstat.gov.by/osids/rubric-info/10306000003](https://dataportal.belstat.gov.by/osids/rubric-info/10306000003) (дата обращения: 10.07.2025)).

7. *Ундозерова, А. Н.* Информационная культура курсанта в условиях цифровой трансформации общества / А. Н. Ундозерова // Понятийный аппарат педагогики и образования : сб. науч. тр. / Благовещ. гос. пед. ун-т. – Благовещенск, 2023. – Вып. 13 / редкол.: М. А. Галагузова (отв. ред.) [и др.]. – С. 259–269.

8. *Эльтемеров, А. А.* Культура поведения в современном цифровом пространстве / А. А. Эльтемеров, О. В. Эльтемерова // Культура и безопасность. – 2021. – № 2. – С. 39–43.

Дата паступлення артыкула ў рэдакцыю: 13.10.2025.