УДК 343.9

**Ковальчук Валерия Руслановна**

студент
Московская академия Следственного комитета
Москва, Россия
lera.kow@mail.ru

**Valeria R. Kovalchuk**

student
Moscow Academy of the Investigative Committee
Moscow, Russia

# МОНИТОРИНГОВАЯ СИСТЕМА «ОКУЛУС» КАК ТЕХНИКО-КРИМИНАЛИСТИЧЕСКОЕ СРЕДСТВО ОБНАРУЖЕНИЯ, ФИКСАЦИИ И ОБРАБОТКИ ЗАПРЕЩЁННОЙ ИНФОРМАЦИИ В СЕТИ ИНТЕРНЕТ[1]

# MONITORING SYSTEM "OCULUS" AS A TECHNICAL AND FORENSIC MEANS OF DETECTING, RECORDING AND PROCESSING PROHIBITED INFORMATION ON THE INTERNET

**Аннотация**

В статье рассматривается мониторинговая система "Окулус" как технико-криминалистическое средство обнаружения, фиксации и обработки запрещённой информации в сети интернет. Описываются особенности работы системы, её возможности и преимущества в сравнении с аналогами. Также обсуждаются этические аспекты использования таких систем.

***Ключевые слова:***

Окулус, мониторинговая система, технико-криминалистическое средство, запрещённая информация, интернет, этика

**Abstract**

The article considers the monitoring system "Oculus" as a technical and forensic means of detecting, recording and processing prohibited information on the Internet. The features of the system, its capabilities and advantages in comparison with analogues are described. The ethical aspects of using such systems are also discussed.

***Keywords:***

Oculus, monitoring system, technical and forensic means, prohibited information, Internet, ethics

В настоящее время сеть Интернет является важным и неотъемлемым элементом жизни людей, а также является основным инструментом обмена информацией. Однако, с ростом числа пользователей Интернета появилась возможность распространения запрещенной информации, включая материалы, которые нарушают законы Российской Федерации [1].

Во-первых, существует растущая потребность в защите от киберугроз и обеспечении безопасности в сети Интернет. Это связано с увеличением количества интернет-пользователей и расширением функционала веб-технологий. Следовательно, важность мониторинговых систем, способных обнаруживать и фиксировать запрещенную информацию в Интернете, увеличивается.

Во-вторых, система "Окулус" была разработана с целью борьбы с распространением запрещенной информации в сети Интернет. В связи с этим, оценка

[1] Научный руководитель: **Кравцов Дмитрий Александрович**, доцент кафедры уголовного права и криминологии Московской академии Следственного комитета, кандидат юридических наук, доцент, подполковник юстиции, г. Москва

ее эффективности, а также возможности для ее усовершенствования могут иметь значительное практическое значение.

В-третьих, в последние годы были введены новые законодательные акты, которые вводят дополнительные требования к операторам связи и поставщикам интернет-услуг в области контроля за распространением запрещенной информации. Таким образом, проведение исследования по эффективности системы "Окулус" может помочь операторам связи и поставщикам интернет-услуг в соблюдении законодательных требований и улучшении своей работы.

Исходя из вышеперечисленных факторов, можно заключить, что исследование по теме является актуальным и имеет практическое значение в свете актуальных вызовов, связанных с обеспечением безопасности в сети Интернет.

В связи с этим, была создана мониторинговая система под названием "Окулус", которая является технико-криминалистическим средством для обнаружения, фиксации и обработки запрещенной информации в сети Интернет.

Мониторинговая система «ОКУЛУС» основана на технологиях анализа текстов и обработки естественного языка. Она используется для обнаружения и фиксации запрещённой информации в сети интернет, такой как насилие, экстремизм, порнография, нарушения авторских прав, а также для поиска информации о преступлениях и незаконных действиях.

Принцип работы системы заключается в автоматическом анализе контента, который загружается в интернет, и в поиске ключевых слов и фраз, связанных с запрещённой информацией. В случае обнаружения подозрительного контента система отправляет его на дополнительную проверку экспертам, которые принимают решение о том, является ли он запрещённым или нет [2].

Система «ОКУЛУС» также использует алгоритмы машинного обучения для улучшения своей работы и распознавания новых форм запрещённой информации. Это позволяет системе быть более эффективной и точной в своих решениях [3].

Мониторинговая система "Окулус" может передавать информацию правоохранительным органам в нескольких форматах, в зависимости от требований и возможностей конкретной системы и органов.

Одним из способов передачи информации является автоматическая отправка отчетов о запрещенной информации с указанием времени и места ее обнаружения.

Такие отчеты могут быть направлены на специальный сервер правоохранительных органов или на электронную почту ответственных сотрудников.

Еще одним способом является предоставление доступа к базе данных системы "Окулус" для правоохранительных органов. В этом случае сотрудники органов могут самостоятельно производить поиск запрещенной информации в базе данных системы.

Также возможно передача информации о конкретных случаях обнаружения запрещенной информации в формате электронного сообщения с подробным описанием события, включая информацию о времени, месте и характере обнаруженной информации.

В любом случае передача информации осуществляется в соответствии с законодательством Российской Федерации о защите персональных данных и иных нормативных актов, регулирующих деятельность правоохранительных органов.

Для обработки информации в системе "Окулус" применяется не менее чем 48 серверов, оснащенных современными графическими ускорителями высокой производительности. Распознавание информации происходит путем применения нейронных сетей, основанных на технологии глубокого машинного обучения. Как пояснил Константин Буланов, директор по цифровым технологиям Государственного Радиочастотного Центра (ГРЧЦ), система способна выявлять запрещенные материалы на нескольких кадрах видеофрагментов, в сложных рукописных текстах и рисованном контенте. В настоящее время рассматривается возможность добавления новых типов нарушений и функции определения поз людей и их действий. Планируется проработать эти возможности до 2025 года.

Российские разработки в области отслеживания опасного контента не являются уникальными. Подобные системы и сервисы существуют и в других странах мира. Например, США работают с этими вопросами на разных уровнях, как внутри страны, так и на международном уровне, с 1942 года, будучи членом так называемого альянса «Пять Глаз». Была создана специальная инфраструктура с центрами накопления и обработки информации. В настоящее время разрабатываются решения для автоматизации мониторинга сетей. Специальные подразделения, такие как Исследовательское агентство США по развитию интеллекта (IARPA) и Киберкомандование США (US CYBERCOM), занимаются проблемами национальной кибербезопасности. В Китае также действует несколько научно-исследовательских институтов и 12 оперативных бюро, включая Министерство общественной

безопасности (МОБ) и Министерство государственной безопасности (МГБ), ответственные за организацию и проведение радиоэлектронной борьбы и контроль информационных каналов, в том числе обнаружение и перехват сведений, подрывающих информационную безопасность страны. Наиболее известные китайские проекты в этой области — это "Система социального кредита" и проект "Золотой щит" [4].

В Великобритании также существует несколько государственных органов, включая Национальную кибер-силу (National Cyber Force - NCF), Управление связи правительства (GCHQ) и Центр национальной кибербезопасности (NCSC), которые занимаются всеми видами кибероперaций. Они используют различные системы мониторинга и контроля, такие как Optic Nerve. Кроме того, в стране создан государственный медиарегулятор Ofcom, который контролирует деятельность всех телекоммуникационных компаний без исключения.

В то же время необходимо сказать о том, что мониторинговая система «Окулус» также позволяет осуществлять предупредительную деятельность следователям следственного комитета. В частности, использование мониторинговой системы может предоставить следователям следственного комитета следующие предупредительные возможности:

1. Раннее обнаружение потенциальных угроз. Система позволяет мониторить определенных лиц, идентифицировать необычную или подозрительную активность и раньше времени обнаруживать потенциальные угрозы. Это может помочь предотвратить планируемые преступления или террористические акты.

2. Обнаружение связей и сетей. Мониторинговая система «Окулус» позволяет анализировать данные и выявлять связи между различными лицами, организациями или группами. Это помогает строить картину событий и раскрывать сложные преступные схемы, а также идентифицировать ключевых участников.

3. Предупреждение о возможных преступлениях. Анализ данных, собранных системой «Окулус», может позволить выявить предвестники преступлений или намеки на планируемые действия. Следователи могут оперативно реагировать на такие предупреждения, предпринимая соответствующие меры для предотвращения преступлений или минимизации их последствий.

4. Мониторинг опасных мест и событий. Система может быть настроена для мониторинга определенных локаций или массовых мероприятий, где существует

повышенный риск возникновения преступлений или инцидентов. Следователи могут получать предупреждения о подозрительной активности или нарушениях, чтобы принять меры по обеспечению безопасности и предотвращению преступлений.

*Использование мониторинговой системы «Окулус» может предоставить следователям следственного комитета ценные предупредительные возможности в борьбе с преступностью в эпоху развития цифровых технологий. Эта технология позволяет обнаруживать подозрительную активность, выявлять связи и сети, предупреждать о возможных преступлениях и мониторировать опасные места и события. Однако при использовании «Окулус» следователям следует учитывать законодательство о приватности и правах человека, а также соблюдать баланс между безопасностью и приватностью. Кроме того, сотрудничество с другими органами правопорядка, профессиональное обучение и развитие являются важными аспектами для эффективного использования мониторинговой системы «Окулус».*

В результате исследования можно сделать вывод, что мониторинговая система «окулус» представляет собой высокотехнологичное технико-криминалистическое средство обнаружения, фиксации и обработки запрещенной информации в сети интернет. Она позволяет оперативно и эффективно выявлять различные виды нарушений, в том числе связанные с нарушением правил дорожного движения, контрабандой товаров, распространением запрещенной информации и террористической деятельностью.

Однако, необходимо отметить, что использование мониторинговой системы «окулус» должно осуществляться с учетом прав человека на защиту личной жизни и конфиденциальность персональных данных. Поэтому, важно соблюдать законодательные нормы и процедуры при использовании данной системы в деятельности органов внутренних дел и других государственных структур.

В целом, мониторинговая система «окулус» является эффективным инструментом борьбы с преступлениями и обеспечения безопасности общества в сети интернет. Однако, для успешного применения данной системы необходимо постоянное совершенствование технологий и процедур работы, а также соблюдение законодательных норм и правил при ее использовании.

## Список использованных источников

1. Бронников И.А., Закальский Г.В. Цифровой двойник в политическом процессе современной России // PolitBook. 2021. №3. URL: https://cyberleninka.ru/article/n/tsifrovoy-dvoynik-v-politicheskom-protsesse-sovremennoy-rossii (дата обращения: 26.04.2023).

2. СМИ: Роскомнадзор запустил интеллектуальную систему отслеживания незаконного контента в интернете «Окулус». URL: https://habr.com/ru/news/716464/ (Дата обращения: 26.04.2023 г.).

3. Что такое "Окулус" и зачем он нужен Роскомнадзору? URL: https://rg.ru/2023/02/13/chto-takoe-okulus-i-zachem-on-nuzhen-roskomnadzoru.html (Дата обращения: 26.04.2023 г.).

4. Что такое «Окулус». Как Роскомнадзор использует новую систему слежки. URL: https://zakonguru.com/izmeneniya/sistema-okulus.html (Дата обращения: 26.04.2023 г.).