

является аналитика безопасности. Посредством высоких скоростей вычислительных процессов интеллектуальные технологии предоставляют аналитикам возможность в автоматическом режиме производить расследование признаков заражения и получать закономерности. Данного рода система основывается на объединении данных из журналов событий и многотысячных сетевых потоков.

Также на сегодняшний день происходят активные разработки интеллектуальных решений из области кибербезопасности, позволяющих в автоматическом режиме реагировать на атаки и управлять защитой. ИИ позволяет координировать и автоматизировать многочисленные меры противодействия, которые обычно выполняются в присутствии человека. Как пример можно отметить решение IBM Security SOAR (Security Orchestration, Automation and Response – платформы оркестрации, автоматизации и реагирования на киберинциденты), формирующее единый интеллектуальный центр оперативного и гибкого реагирования.

Помимо этого, предпринимаются попытки разработки унифицированного управления мобильными устройствами и конечными точками. Эта технология предполагает разработку единой платформы, позволяющей производить контекстные и сравнительные анализы,

необходимые для понимания событий безопасности и защиты конечных точек. Сдерживание угроз и управление данными в данном случае производится посредством первого и единственного в данной отрасли решения для унифицированного управления конечными устройствами (UEM – Unified endpoint management), основанного на работе интеллектуальных технологий¹.

Как видно, интеграция ИИ в решении вопросов кибербезопасности предоставляет возможность выявлять подозрительные действия и принимать эффективные меры, тем самым предотвращая нарушения в работе бизнес-систем. В заключение необходимо отметить, что технологии искусственного интеллекта самообучаются на огромном массиве данных, совершенствуя свои «знания» и «понимая» угрозы и риски для кибербезопасности. ИИ выполняет анализ взаимосвязей колоссального количества данных в считанные секунды, посредством чего аналитики намного быстрее реагируют на угрозы относительно традиционных инструментов. ИИ избавляет от длительных исследований и предоставляет уже готовый анализ рисков, сокращая время, необходимое аналитикам для принятия ключевых решений и согласованного устранения угрозы.

Панов С.Л.,

кандидат юридических наук
ветеран МВД России (Омск)

Урусов А.А.

Омская академия МВД России

Аспекты защиты сотрудников органов внутренних дел от клеветнической информации в сети Интернет

В своей повседневной деятельности сотрудники органов внутренних дел (далее – ОВД) осуществляют защиту жизни,

здоровья, прав и свобод граждан, противостоят преступности, охраняют общественный порядок, обеспечивают

¹ Загарских Е.Ю., Загарских Ю.А. Применение кибербезопасности и использование искусственного интеллекта в медицине // Системный анализ в проектировании и управлении : сборник научных трудов XXIII международной научно-практ. конф., Санкт-Петербург, 10-11 июня 2019 года. СПб.: Санкт-Петербургский политехнический университет Петра Великого, 2019. С. 425-429.

безопасность общества и государства. Сотрудники ОВД (полиции) – это категория правоохранителей, которым в ходе исполнения служебных обязанностей приходится сталкиваться с гражданами, зачастую не согласными с законными действиями последних. Нередко часть таких граждан «в отместку» умышленно распространяют заведомо неправдоподобную информацию о событиях (фактах) личной жизни сотрудником полиции, его служебной деятельности и (или) о якобы совершенных ими конкретных противоправных деяниях, в том числе тяжких¹.

Клевета на сотрудников полиции с целью оказания на них давления – достаточно частое явление, особенно на стадии дознания и следствия, когда виновные лица, шантажируя распространением заведомо ложной информации, пытаются таким образом в дальнейшем воздействовать на принятие процессуальных решений в интересах правонарушителей.

Под распространением сведений, порочащих честь и достоинство другого лица, следует понимать опубликование такой информации в печати, трансляцию по радио и телевидению, демонстрацию в кинохроникальных программах, публичных выступлениях. В настоящее время правонарушителями клеветническая информация о сотрудниках ОВД распространяется с использованием информационно-телекоммуникационных технологий, в частности сети Интернет. Интернет-клевета на сотрудников ОВД может осуществляться следующим образом: размещение клеветнических постов пользователями социальных сетей «Одноклассники», «ВКонтакте», «Фейсбук» и других (троллинг); публикация унижительных комментариев на различных интернет-площадках; размещение в сети для публичного доступа фотографий, видеоконтента, порочащих репутацию полицейского; отправка сообщений с унижительным содержанием.

Поводом для клеветы является желание опорочить сотрудника ОВД, унижить его достоинство, создать о нем (например, неэтичное поведение в быту) или его деятельности (например, злоупотребление властью) негативное общественное мнение. Умысел правонарушителя состоит в заведомой ложности размещенных в сети Интернет сведений путем донесения их до третьего лица или неопределенного круга людей².

Действия граждан, связанные с размещением в сети Интернет заведомо ложной информации в отношении сотрудников ОВД, квалифицируются по ч. 2 ст. 128.1 УК РФ – клевета, содержащаяся в публичном выступлении, публично демонстрирующемся произведении или средствах массовой информации. Кроме того, за распространение в средствах массовой информации клеветы в отношении следователя и лица, производящего дознание, предусмотрена уголовная ответственность по ст. 298.1. УК РФ.

Состав преступления является формальным – клевета окончена с момента распространения указанных сведений вне зависимости от того, причинили они какой-либо вред охраняемым законом интересам сотрудника ОВД. Распространяемые при клевете сведения должны в деталях либо в общих чертах характеризовать какой-либо конкретный факт, при этом они могут прямо указывать на событие или содержать косвенную информацию о нем. Заявления общего характера (например, «взяточник», «коррупционер»), не содержащие указания на определенный заведомо ложный факт, не образуют состава клеветы.

Клевета может состоять в распространении заведомо ложных сведений как в отношении конкретного работника полиции, так и в адрес нескольких правоохранителей. В последнем случае при установлении единого умысла (единства намерения) содеянное квалифицируется как одно преступление; если же имела место клевета в отношении двух или

¹ Сулейманова И.Е. О защите чести и достоинства представителей власти в сфере порядка управления // Правовое государство. 2016. № 1. С. 82.

² Закирова И.И. Клевета, предусмотренная ч. 2 ст. 128.1 УК РФ: проблемы толкования и правоприменения // Правовая политика и правовая жизнь. 2017. № 4. С. 125.

более лиц, совершенная с различным умыслом и разрывом во времени, содеянное квалифицируется по правилам совокупности преступлений.

Клеветнические сведения могут относиться лишь к фактам прошлого или настоящего деятельности или (и) личной жизни сотрудника ОВД, – измышления о позорящих фактах, которые могут наступить в будущем, состава клеветы не образуют.

За распространение клеветнической информации к уголовной ответственности может быть привлечено любое лицо, достигшее 16-летнего возраста.

Сообщение таких сведений лицу, которого они касаются, не может признаваться их распространением, если лицом, сообщившим данные сведения, были приняты достаточные меры конфиденциальности, с тем чтобы они не стали известными третьим лицам. Кроме того, официальное обращение граждан с претензиями (жалобами) в отношении действий отдельных сотрудников полиции, но не нашедшие подтверждения, не могут служить основанием для привлечения заявителей к уголовной ответственности¹.

Сложность самостоятельного сбора доказательств самим оклеветанным сотрудником полиции вызвана тем, что его возможности, как правило, ограничены в техническом плане. Данные об IP-адресе лица, разместившего порочащие сведения, месте нахождения его компьютера и т.д. можно узнать только в том случае, если имеется соответствующее постановление следователя или суда. К тому же зачастую невозможно установить лицо, распространяющее ложные сведения, если это было сделано, например, путем отправки анонимных писем в адрес МВД или при распространении информации в Интернете лицом, идентифицировать которое невозможно. Большинство лиц,

разместивших в Интернете клеветническую информацию, «прячутся» за вымышленными именами и чужими фотографиями. Вычислить правонарушителя не просто в связи с наличием в сети Интернет эффективных механизмов (например, использование анонимайзеров ToR, SRWare Igon, поддельных адресов электронной почты и пр.) обеспечения анонимности лица, распространившего клеветнические сведения в отношении сотрудника ОВД.

Процесс собирания доказательств потерпевшим в отношении лица, разместившего клеветнические сведения в сети Интернет, довольно затратный как в организационно-техническом смысле (сбор информации об аккаунте, IP-адресе гражданина, оставившего клеветнический пост в социальной сети, владельце сайта), так и в силу материальных затрат, связанных с оплатой досудебной экспертизы и работы нотариуса по нотариальному осмотру, копированию (скриншот) и визированию соответствующей интернет-страницы².

В целях обеспечения надлежащей защиты чести, достоинства и деловой репутации сотрудников, федеральных государственных гражданских служащих и работников, деловой репутации ОВД Главным управлением МВД России по городу Москва принят приказ от 29 июня 2012 г. № 637³. В соответствии с положениями приказа сотрудники правовых подразделений могут оказывать квалифицированную консультационную, методическую и практическую помощь сотрудникам ОВД по вопросам составления искового заявления, порядка его предъявления в суд, обжалования и т.д. При наличии достаточных оснований представитель ОВД может выступать в процессе на стороне истца в качестве третьего лица.

¹ Ребрый В.А., Черепанов П.Ф. Практика работы пресс-служб органов внутренних дел с критическими публикациями в отношении полиции в средствах массовой информации // Закон и право. 2016. № 6. С. 126.

² Артебякина Н.А. Протокол осмотра нотариусом интернет-страницы как средство обеспечения доказательств в гражданском судопроизводстве // Вестник гражданского процесса. 2019. № 1. С. 275.

³ О порядке взаимодействия подразделений системы ГУ МВД России по г. Москве при осуществлении защиты чести, достоинства и деловой репутации органов внутренних дел и организаций системы ГУ МВД России по г. Москве : приказ ГУ МВД России по городу Москве от 29.06.2012 № 637. URL: <https://www.yao.msk.mvd.rf> (дата обращения: 11.01.2022).

По мнению автора, существующие нормы закона при их активном и последовательном применении вполне могут обеспечить неотвратимость наказания за клевету в отношении сотрудников органов внутренних дел в сети Интернет. Кроме того, ст. 152 Гражданского кодек-

са РФ предоставляет в качестве способов защиты чести и достоинства или деловой репутации право требовать опровержения таких сведений, причем если сведения распространены в Интернете, то и опровержение должно быть размещено именно на сайтах Сети.

Становая О.В.

Волгоградская академия МВД России

Криминологическая характеристика преступлений, совершаемых мигрантами

Проблема незаконной миграции и совершения мигрантами преступлений в России на сегодняшний день является довольно серьезной государственной проблемой. Для ее решения была принята Концепция государственной миграционной политики Российской Федерации на период до 2025 года, утвержденная Президентом РФ 13 июня 2012 г.

К основным направлениям миграционной политики Российской Федерации в области противодействия незаконной миграции относятся: совершенствование правовой базы противодействия незаконной миграции, совершенствование мер ответственности за нарушение миграционного законодательства Российской

Федерации, противодействие организации каналов незаконной миграции, в том числе за счет повышения защищенности паспортно-визовых и иных документов, позволяющих идентифицировать личность, совершенствование межведомственного взаимодействия, в том числе обмена информацией на внутригосударственном уровне, а также с компетентными органами иностранных государств по вопросам противодействия незаконной миграции и т.д.¹

Согласно статистике ГИАЦ МВД России, за период с января 2016 г. по декабрь 2020 г. совершено преступлений иностранными гражданами и лицами без гражданства:

Преступления, совершенные иностранными гражданами и лицами без гражданства	Год				
	2020	2019	2018	2017	2016
Всего	34400	34917	38598	41047	43933

Как видно из таблицы, количество преступлений из года в год снижается, что, безусловно, является хорошим показателем. Однако цифра в 34400 совершенных преступлений все равно является для России значительной, тем более что в таблице не учитывались зарегистрированные преступления, совершенные в отношении иностранных граждан и лиц без гражданства, которые также исчисляются десятками тысяч².

Исследование преступлений, связанных с мигрантами в Российской Федерации, позволило установить самые распространенные правонарушения, совершаемые гражданами иностранных государств:

– тяжкие преступления против личности: изнасилования, умышленное причинение тяжкого и легкого вреда здоровью, убийства, побои, действия сексуального характера, истязания,

¹ Концепция государственной миграционной политики Российской Федерации на период до 2025 года. URL: <https://www.garant.ru/products/ipo/prime/doc/70088244/> (дата обращения: 14.01.2022).

² Статистические сведения по миграционной ситуации. URL: <https://xn--b1aew.xn--p1ai/Deljatelnost/statistics/migracionnaya> (дата обращения: 16.01.2022).