уже, как я сказал, полномасштабная информационная война за умы наших людей, за будущее наших детей. Мы проиграть эту войну не можем. У нас хорошее исходное положение, поэтому мы и не должны ее проиграть. Вижу, как мы все чаще перехватываем повестку в Интернете, но говорить, что наша информация там доминирует, что мы там побеждаем пока, наверное, преждевременно... Надо быть взвешенными, развивать свои ресурсы. А мы это умеем делать! Ну и кадры – человеческий потенциал. Нужно, сохраняя журналистские коллективы, находить новых людей, молодых, креативных. И самое главное, патриотично настроенных!».

Несмотря на стабилизировавшуюся общественно-политическую обстановку в Республике Беларусь, беглые оппозиционеры, подконтрольные специальным службам недружественных нам государств, до настоящего времени продолжают использовать природоохранную тематику в попытках создания очагов социальной напряженности в обществе, ослабления авторитета власти, системы государственного управления, основ национальной государственности. Активно используются современные технические средства коммуникации, информационные ресурсы, позволяющие мгновенно распространять недостоверную, искаженную информацию и тем самым оказывать целенаправленное деструктивное информационное воздействие как на широкие слои населения, так и отдельные категории граждан.

Одним из широко используемых нашими противниками в информационном пространстве направлений является «лесная» повестка. Особое место в ней занимает тема «массовые вырубки лесов с целью пополнения госбюджета», которой в информационных ресурсах, признанных экстремистскими материалами, а также иных деструктивных средствах информации, посвящены многочисленные публикации, набравшие сотни тысяч просмотров. Также в целях дискредитации органов власти и управления «раскрутке» со стороны деструктивных информационных ресурсов подвергаются темы: «помилование бывшего министра лесного хозяйства», «остановка пеллетных производств», «обход санкций», «экспорт пилопродукции в азиатские страны по низким ценам», «рост числа лесных пожаров» и др. Таким образом, внешними оппонентами власти посредством подконтрольных информационных ресурсов предпринимаются активные попытки при помощи «лесной» повестки сформировать мнение об «отрыве» государства от проблем народа, ухудшении экономической ситуации, уменьшении социальных гарантий и льгот, отсутствии перспектив, тем самым нарастить в обществе конфликтный потенциал.

Информационное воздействие деструктивного характера в настоящее время является одним из основных элементов формирования протестных настроений как у работников лесной отрасли, так и широких слоев населения, фактором, способствующим их вовлечению в экстремистскую и иную противоправную деятельность. Складывающаяся социально-политическая обстановка актуализирует научную проработку противодействия рискам, вызовам и угрозам информационного характера в сфере лесного хозяйства.

В Министерстве лесного хозяйства Республики Беларусь разработаны и в ноябре 2020 г. утверждены Методические рекомендации по организации деятельности заместителей руководителей по идеологической работе, а также лиц, ответственных за ведение идеологической работы в организациях, подчиненных Министерству лесного хозяйства Республики Беларусь в рамках реализации изложенных в них мер обеспечения информационной безопасности, ведется активная работа со средствами массовой информации, созданы и развиваются ведомственные интернет-ресурсы, по средствам которых осуществляется объективное информирование о социально значимых явлениях общественной жизни, продвигается позитивная прогосударственная информационная повестка. Таким образом, основной мерой повышения эффективности противодействия деструктивному информационному воздействию со стороны Министерства лесного хозяйства Республики Беларусь является активное наполнение информационного пространства эксклюзивным, отраслевым контентом прогосударственной направленности, позволяющее формировать информационную повестку и доминировать в информационном пространстве.

УДК 343.985.8

Б.В. Ковалик

О НЕКОТОРЫХ ОРГАНИЗАЦИОННО-ПРАВОВЫХ МЕРАХ ПРОТИВОДЕЙСТВИЯ МОШЕННИЧЕСТВАМ, СОВЕРШЕННЫМ С ИСПОЛЬЗОВАНИЕМ ИНФОРМАЦИОННО-КОММУНИКАЦИОННЫХ ТЕХНОЛОГИЙ

Противодействие мошенничествам, совершенным с использованием информационно-коммуникационных технологий, является приоритетным направлением деятельности органов внутренних дел (ОВД). В целях повышения его эффективности остро стоит вопрос разработки новых форм и методов предупреждения и пресечения преступлений, включая меры оперативно-розыскной профилактики (ОРП). Являясь самостоятельной подсистемой социальной профилактики, ОРП имеет сложную структуру и свои отличительные особенности, сущность которой, по мнению Д.Н. Лахтикова, в первую очередь выражается в использовании оперативно-розыскных сил, средств и методов в целях недопущения совершения преступлений.

При планировании и реализации мер ОРП необходимо учитывать специфику отдельных видов преступлений, в частности дистанционных мошенничеств. Оказание активного противодействия сотрудникам оперативных подразделений со стороны злоумышленников и предпринятые ими меры по обеспечению собственной анонимности, выражающиеся в том числе в совершении преступлений из-за пределов Республики Беларусь, затрудняют реализацию индивидуальной ОРП, объектом которой являются конкретные лица. В данной связи видится целесообразным обеспечивать предупреждение дистанционных мошенничеств посредством общей ОРП, воздействуя на причины и условия, способствующие совершению преступлений.

Одним из необходимых условий реализации злоумышленниками ряда распространенных мошеннических схем на территории Республики Беларусь является функционирование в национальном сегменте сети Интернет фишинговых сайтов.

Данные ресурсы представляют собой подложную копию легитимно существующего сайта, созданную с целью введения пострадавшего в заблуждение. Очевидным признаком, выдающим преступный замысел, является адрес ресурса, который, как правило, создается по подобию реального URL для минимизации подозрений у потенциальной жертвы.

Установление членов преступных групп, использующих подобные мошеннические схемы, и, следовательно, возврат денежных средств, похищенных злоумышленниками, по названным выше причинам осуществить весьма затруднительно. В данной связи действенной мерой предупреждения фактов совершения хищений данным путем является оперативный поиск указанных ресурсов и их последующая превентивная блокировка.

В настоящий момент данная деятельность осуществляется подразделениями по противодействию киберпреступности криминальной милиции МВД Республики Беларусь. Однако в процессе реализации указанного механизма возникает ряд трудностей, вызванных различными факторами. Во-первых, в связи с автоматизацией мошенниками процесса генерации фишинговых ссылок для их своевременного поиска в необходимом объеме требуется задействовать значительное количество сотрудников. Во-вторых, в настоящее время процедура блокировки мошеннических Интернет-ресурсов занимает большой промежуток времени, в среднем от 7 до 14 рабочих дней с момента направления сведений о его выявлении в уполномоченные органы.

На основании изложенного, следует констатировать, что действующий порядок ограничения доступа к фишинговым ресурсам является малоэффективным. Наличие данных обстоятельств приводит к увеличению числа пострадавших от преступных действий мошенников. В целях повышения эффективности реализации указанного алгоритма, видится целесообразной разработка мер как организационно-тактического, так и правового характера.

Для осуществления оперативного поиска фишинговых Интернет-ресурсов, а также с целью рационального использования сил оперативных подразделений ОВД, на наш взгляд, имеется необходимость автоматизации данных процессов посредством использования специализированного Интернет-ресурса DNS Twist, который самостоятельно осуществляет поиск возможных вариантов искажения URL реальных ресурсов при создании фишингового сайта. В случае положительного поискового результата сканер фишинговых доменов самостоятельно осуществляет их первичный анализ: определяет IP-адрес, name- и mail-серверы.

Дальнейшее совершенствование указанного алгоритма возможно посредством внедрения нейросетевых алгоритмов, самостоятельно осуществляющих поиск криминогенных объектов в сети Интернет. Реализация данного предложения позволит минимизировать непосредственное участие оперативных сотрудников в данном процессе. При выборе архитектуры искусственного интеллекта для решения классификационной задачи, которой, по сути, является отнесение тех или иных сайтов к категории фишинговых, возможно использование сверточных, рекуррентных или комбинированных нейронных сетей.

Обучение и тестирование компьютерных алгоритмов возможно путем использования уже собранных сотрудниками сведений о фишинговых сайтах, а также информации о легальных ресурсах, которые могут представлять интерес для преступников. К ним можно отнести Интернет-порталы банковских и финансовых организаций, почтовых и курьерских сервисов, Интернет-магазины и т. п. Это позволит алгоритмам самостоятельно определять поисковые признаки, а также выявлять общие тренды и изменения в методах, используемых мошенниками, в целях адаптации модели к новым угрозам и минимизации ложных поисковых результатов.

При наличии достаточных вычислительных мощностей, как поисковые признаки возможно использовать не только сведения об адресе ресурса, но и об их содержательной и визуальной составляющей. Данная мера повысит эффективность их выявления, так как сведения, содержащиеся на фишинговом сайте, мошенники излагают практически без изменений, поскольку это играет определяющую роль при введении пострадавшего в заблуждение. В целях эффективного документирования факта выявления фишингового ресурса необходимо предусмотреть возможность не только копирования его IP-адреса, URL и т. п., но и запечатления интерфейса (скриншота).

В последующем инструменты мониторинга могут быть интегрированы с системой блокировки, осуществлять которую уполномочено Республиканское унитарное предприятие по надзору за электросвязью «БелГИЭ» по указанию Министерства связи и информатизации Республики Беларусь. Платформу для оперативной передачи сведений указанным субъектам со стороны МВД возможно организовать путем расширения функционала имеющихся ведомственных автоматизированных информационных систем.

Для реализации данных предложений соответствующих изменений также требует правовая регламентация процесса блокировки указанных ресурсов. В настоящий момент ограничение доступа к Интернет-ресурсам осуществляется в соответствии с основаниями, предусмотренными ст. 51^1 Закона Республики Беларусь «О средствах массовой информации» (далее – Закон о СМИ). Действующая редакция закона не содержит положений, предусматривающих блокировку ресурсов глобальной компьютерной сети, реализация которых может быть возложена на Министерство внутренних дел Республики Беларусь (МВД). В данной связи, прежде чем направить идентификаторы фишинговых сайтов субъекту, осуществляющему блокировку, сотрудники ОВД вынуждены предварительно обращаться в иные ведомства, что негативно сказывается на оперативности реализации данной процедуры.

На основании изложенного полагаем возможным заключить, что в настоящее время имеется обоснованная необходимость автоматизации поиска ресурсов сети Интернет, используемых в преступных целях, а также внесения соответствующих изменений в ст. 51^1 Закона о СМИ, наделяющих МВД правом принятия решения об их блокировке. Реализация данной инициативы может быть полезна не только в решении задач по противодействию дистанционным мошенничествам и иным киберпреступлениям, но и иных задач, возложенных на различные подразделения ОВД Республики Беларусь.