нарушителей, предупредить о проблемах с соблюдением общественного порядка, предсказать наиболее неблагополучные территории и так далее. В результате деятельность правоохранительных органов становится более эффективной.

Несмотря на многочисленные преимущества, интеграция искусственного интеллекта в работу полиции может создать ряд рисков.

Первым и наиболее значимым является перспектива нарушения конфиденциальности.

Нельзя не отметить проблемы профилирования: искусственный интеллект в случае его неудачного обучения или наличия индивидуального мнения у создателя способен демонстрировать ложную связь между различными элементами.

Исходя из рассмотренных в рамках данного материала направлений развития применения искусственного интеллекта можно предложить следующее:

1) проведение мероприятий по расширению применения искусственного интеллекта в органах внутренних дел с учетом специфики деятельности подразделений;

2) допуск к разработке и обучению программ с искусственным интеллектом только высококвалифицированных специалистов;

3) проведение обязательного тестирования разработанных и обученных систем перед их широким применением на практике;

4) проработка возможности разработки программ дополнительного профессионального обучения лиц, способных эффективно использовать программное обеспечение с искусственным интеллектом.

Кошкина В.В.

Владивостокский филиал
Дальневосточного юридического института МВД России им. И.Ф. Шилова

Криминологические меры противодействия преступлениям, совершаемым с использованием компьютерных и телекоммуникационных технологий

Качественное и своевременное реагирование государства на изменение структуры и характера преступности является первостепенной задачей для обеспечения прав и свобод человека и гражданина. В современной действительности, где технологические возможности с каждым днем развиваются и становятся более сложными, необходимо принимать все необходимые меры для противодействия преступности, особенно с использованием информационных технологий.

Предупреждение и профилактика преступлений – ключевые аспекты в предотвращении преступности и ее ликвидации.

К основным направлениям противодействия компьютерной преступности относится, разумеется, ее профилактика.

Кроме того, расследование компьютерной преступности может существенно упроститься, если преодолеть ее латентность, например, посредством реализации следующих мер.

Во-первых, это применение статистических методик выявления. К ним относятся опросы пользователей персональных ЭВМ, мониторинг СМИ на предмет соответствующих публикаций. Показательно, что некоторые авторы относят к числу направлений совершенствования борьбы с киберпреступностью создание качественной научной базы. Однако, во-первых, научная база необходима для исследования всей преступности и противодействия всем преступлениям, а не только рассматриваемой нами категории и, во-вторых, практически их предложения сводятся к повышению качества сбора криминологической информации и созданию некой единой информационной базы, позволяющей обмениваться этой информацией и вырабатывать общие меры. Иначе говоря, все суждения о научной базе сводятся к созданию криминалистических методик расследования и криминологических методик противодействия данной группе преступлений.

Во-вторых, это применение бухгалтерских методов анализа результатов предпринимательской деятельности хозяйствующих субъектов.

В-третьих, это правовая пропаганда, массовая информация населения об опасностях компьютерной преступности.

В-четвертых, это изменение статистических правил учета компьютерной преступности, выделение ее в отдельную графу статистической отчетности правоохранительных органов.

В-пятых, это рост профподготовки сотрудников дознания и следствия, в частности, предлагается ввести специальные курсы повышения квалификации сотрудников ОВД в части изучения методики расследования компьютерных преступлений.

Ряд авторов полагают необходимым включение в число криминологических мер противодействия развитие правоприменительной деятельности, внедрение в нее новейших способов борьбы с компьютерными преступлениями[1]. Однако и это направление, помимо слишком общего характера, сводится в конечном счете к подготовке методических рекомендаций для сотрудников правоохранительных органов. И.Н. Архипцев, А.В. Сарычев,

[1] Напр.: Пархоменко С.В., Евдокимов К.Н. Предупреждение компьютерной преступности в Российской Федерации: интегративный и комплексный подходы // Всероссийский криминологический журнал. 2015. № 2. С. 272.

Р.В. Красников[1] в числе мер, способных повысить профессионализм сотрудников в борьбе с данной категорией преступлений, предлагают обучение по специальной образовательной программе «Информационная безопасность». С таким расширением подготовки специалистов по данной категории преступлений следует согласиться: очевидно, отдельного спецкурса или отдельного учебного предмета для противодействия преступлениям, которые в настоящее время имеют явную тенденцию к росту, уже недостаточно.

Наряду с отдельной образовательной программой, целесообразным было бы повышение квалификации действующих сотрудников правоохранительных органов на курсах повышения квалификации.

В-шестых, перспективным направлением представляется переход от территориального принципа расследования данных преступлений к функциональному принципу. Иначе говоря, необходимым представляется создание в системе МВД России отдельного и специального органа, в функции которого входило бы противодействие киберпреступности. В этом случае решается и проблема сбора и обработки сведений о таких преступлениях и их систематизации, создания единой базы данных о них, создания единой методики их расследования, секретность которой вряд ли можно обеспечить в условиях, когда к ней может обратиться каждый дознаватель или следователь, действующий по территориальному принципу подследственности.

В-седьмых, это создание программных комплексов и баз данных. Следует отметить, что в настоящее время ОВД используются ИБД-Ф «Дистанционное мошенничество».

С.Л. Катаев добавляет к указанному выше ряд социальных факторов, необходимых для учета в противодействии компьютерной преступности. Социологическая суть его позиции состоит в том, что ныне наше общество «замахнулось» на постмодернизацию, однако в нем еще чрезвычайно сильны традиционные элементы. Например, он отмечает, что «постмодернизация проявляется в активном использовании компьютерной техники, а элементы предшествующих стадий развития проявляются в примитивном воровстве. Нет необходимых нравственных образцов. Для решения этой проблемы необходим этический кодекс компьютерного сообщества, который бы закрепил нормы обращения с компьютерной информацией, сформировал основы корпоративной морали и информационной ответственности»[2].

С точки зрения общесоциальных факторов, важное практическое значение имеет и стоимость экспертизы: по данной категории дел она оказы-

[1] Архипцев И.Н., Сарычев А.В., Красников Р.В. Совершенствование подготовки сотрудников органов по противодействию преступлениям, совершаемым с использованием информационных технологий // Legal Concept. 2020. №2. С.159.

[2] Цит. по: Коликов Н.Л. Причины и условия профессиональной компьютерной преступности // Вестник Южно-Уральского государственного университета. Серия: Право. №19 (236). 2011. С. 32.

вается достаточно высокой. Так, выделяются 4 основных вида, соответствующие четырем основным объектам экспертизы: аппаратно-компьютерная, направленная на все существующие ПК, вспомогательные устройства, их составляющие, аппаратные средства и т.п.; программно-компьютерная, направленная как на системное, так и прикладное программное обеспечение ПК; информационно-компьютерная, направленная на анализ метаданных, баз данных и отдельных файлов, списков, иных информационных массивов, видеоизображений, текстов и т.п.; компьютерно-сетевая, направленная на сетевое оборудование и переносные электронные устройства (как правило, планшеты и сотовые телефоны).

Минимальная цена такой экспертизы – 15000, максимальная, необходимая для комплексного анализа инцидента, – 300 тысяч рублей[1], что для среднего потребителя в России сложно изыскать даже под угрозой наступления уголовной ответственности. Во Владивостоке такие услуги оказывают крайне ограниченный перечень учреждений: Центр экспертиз при Институте судебных экспертиз и криминалистики, Научно-исследовательский институт экспертиз, Федерация судебных экспертов.

В этой связи обоснованным представляется развитие частных организаций, направленных на доказывание компьютерных преступлений. Как отмечают специалисты, «на Западе такие компании давно заняли свой сегмент на рынке безопасности. При этом основными направлениями рынка компьютерных исследований в России и в мире являются: реагирование на инциденты (Incident response); расследование инцидентов (eDiscavery); компьютерная диагностика (Digital Forensis); мониторинг инцидентов; юридическое сопровождение инцидентов»[2]. При этом наибольшее значение для доказывания имеют направление расследования инцидентов (позволяющий ответить на вопросы о том, почему и каким образом случился инцидент, кто причастен к его совершению и каков порядок действий должен быть со стороны потерпевшего), связанное с определением обстоятельств инцидента и формированием гипотез (следственных версий), а также реагирование на инциденты, позволяющее точно действовать в ситуации продолжения инцидента, без нарушений собрать доказательства. Эти же авторы упоминают термин «компьютерная криминалистика», сводящаяся, по их мнению, в большинстве случаев к непроцессуальной деятельности по анализу скомпроментированных объектов (компьютерной информации, компьютеров, их сетей, средств связи и т.п.). Пока же, возможно, наиболее правильным решением было бы

[1] Компьютерно-техническая экспертиза // Российский экспертный фонд «Техэко». URL: https://expert-center.ru/kompyuterno-tekhnicheskaya-ekspertiza (дата обращения: 10.09.2025).

[2] Смирнова И.Г., Сачков Д.И. Сложности доказывания по делам о преступлениях в сфере компьютерной информации // Криминалистические чтения на Байкале – 2015 / отв. ред. Д.А. Степаненко. Иркутск, 2015. С. 99.

обращение к опыту УПК Турции 2004 г.[1], который в ст. 134-1 закрепляет отдельное и самостоятельное следственное действие: досмотр компьютеров, компьютерных программ и изъятие записей. Такой подход, как представляется, позволил бы развить уголовно-процессуальную и криминалистическую науку в новом и специальном направлении, связанном с анализом компьютерных данных и формированием методик доказывания по компьютерным преступлениям.

Итак, для обеспечения эффективной борьбы с преступлениями в сфере информационных технологий необходимо провести масштабную унификацию и систематизацию уголовного закона, выделить отдельную главу, включающую составы преступлений, связанных с информационными технологиями. Кроме того, важно развивать международное сотрудничество, обучение специалистов, усиление ответственности для виновных и активно информировать население о методах защиты информационной безопасности. Только таким образом можно достичь поставленных задач и обеспечить безопасность в информационном пространстве.

Титов Д.В.

Восточно-Сибирский институт МВД России (г. Иркутск)

Шаевич А.А.

Восточно-Сибирский институт МВД России (г. Иркутск)

Интегрированная модель противодействия киберпреступности

В условиях стремительной цифровизации экономики и общественной жизни киберпреступность приобретает все более трансграничный, организованный и технологически изощренный характер. Это ставит перед государствами, организациями и правоохранительными структурами комплексную задачу: обеспечить не только техническую устойчивость информационных систем, но и правовую основу для эффективного взаимодействия в расследовании и пресечении преступлений, совершаемых в виртуальной среде. Актуальность данной проблемы обусловлена фундаментальным противоречием между глобальной природой киберугроз и национальной ограниченностью юрисдикций, что затрудняет сбор, признание и использование цифровых доказательств за пределами одной правовой системы.

Правовые механизмы становятся ключевым элементом обеспечения процессуальной легитимности и международной взаимопомощи. Так, Н.О. Мороз подчеркивает основу подхода ЕС: «В ЕС используется

[1] Уголовно-процессуальный кодекс Турецкой Республики / науч. ред. В.А. Оровер. Владивосток: ДВГУ, 2015. С. 112.