необходимости развития и внедрения подобных технологий в нашей стране. Это позволит не только повысить надежность доступа пользователей к АС дорожной полиции, но и внести значительный вклад в повышение безопасности дорожного движения.

Бондарь К.М.,

кандидат технических наук, доцент
Дальневосточный юридический институт МВД России им. И.Ф. Шилова (г. Хабаровск)

Аспект виктимности в современной киберпреступности России

Развитие информационных технологий стало ключевым фактором в возникновении и распространении киберпреступности. Анализ показывает, что большинство киберпреступников – это высококвалифицированные специалисты, обладающие глубокими знаниями в области IT. Они используют свои навыки для совершения различных преступлений, от мошенничества до угроз национальной безопасности, при этом часто скрывая свое местоположение и действуя из любой точки мира.

Установление личности преступников в сфере интернет-преступности затруднено в связи с дистанционным характером совершаемых деяний[1]. Сложность в этой борьбе заключается в ее скрытом характере, что приводит к низкой раскрываемости. Эффективность раскрытия и расследования таких преступлений напрямую определяется оперативностью обнаружения, а также особенностями и следами, которые, как правило, существуют только в виртуальном пространстве.

Современные информационные технологии открывают широкие горизонты, позволяя использовать инновационные методы торговли и предоставления услуг. Но возможно и попадание на мошенников, маскирующихся под добросовестных продавцов. В Интернете мошенники не всегда сразу стремятся украсть деньги, не всегда все сводится к прямому обогащению. Нередко их цель – это ваши личные данные-логины, пароли, файлы. Получив к ним доступ, они могут шантажировать, вымогать деньги или просто использовать информацию в своих интересах.

При этом используются различные программы, которые предназначены для тайного доступа к носителю информации, без уведомления владельца. К ним можно отнести различные рекламные, троянские, вирусы. Все они нацелены на захват и контролирование информации.

Процесс виктимизация населения на сегодняшний день является одной из актуальных проблем. Потенциальные жертвы сами идут на поводу у

[1] Устинов А.А. Основные проблемы раскрытия и расследования интернет-преступлений // Молодой ученый. 2020. № 49 (339). С. 338-340.

мошенников и попадают в их ловушки. Все может начинаться от каких-либо добровольных пожертвований в ложные фонды и приводить к угрозам вымогательства. Одной из способствующих причин является слабая адаптация к быстро меняющейся информационной среде.

Интернет как мощная платформа стал местом проявления виктимности у людей разных возрастов и социальных групп. Молодежь как наиболее активный пользователь сети особенно подвержена риску. Она в силу недостатка опыта легко поддается манипуляциям и обману, тем самым попадая в ловушки злоумышленников[1].

Следующая группа подверженных киберпреступности – это люди зрелого и пожилого возраста. Освоение Интернета им дается с трудом. Мошенники, часто выдавая себя за специалистов, убеждают в необходимости обновления устройств, жертва, сообщая код или переходя по ссылке, лишается сбережений.

Пенсионные накопления также привлекают мошенников. Они, прикрываясь родственниками, попавшими в беду, или представителями несуществующих благотворительных фондов, пытаются завладеть сбережениями пенсионеров. Социальная изоляция, характерная для одиноких пенсионеров и людей с узким кругом общения, также делает их более уязвимыми.

По результатам ежегодного опроса Банк России составил портрет пострадавшего от кибермошенников. В 2024 г. каждый третий из 10 респондентов сталкивался с разными видами финансового кибермошенничества, при этом 9 % пострадавших лишились денег[2].

Банк России выделил топ-5 способов, как мошенники пытались получить доступ к деньгам. К ним относят: телефонный звонок или СМС-сообщение – 45,6%; атака через мессенджеры – 15,7%; сообщения в социальных сетях – 10,3%, письма на электронную почту – 7,7%. Впервые в пятерке – получение доступа к аккаунтам людей на Госуслугах, что составляет 7%. На остальные каналы мошенничества (фишинговые ресурсы, поддельные QR-коды и прочие) пришлось 13,7%.

Банк России также сообщает о возрастной категории лиц, подверженных стать жертвами, – в большинстве случаев это пожилые люди. Однако статистика показывает: средний возраст пострадавших составляет 25-44 года. Это те, кто проявляет высокую экономическую активность и пользуется банковскими серверами.

В отличие от взлома информационных систем, требующих глубоких знаний в области программирования, современные киберпреступники акцен-

[1] Яценко Т.Е. Психологическая диагностика виктимности как социально-психологического свойства личности // Актуальные проблемы современной науки, техники и образования. 2019. Том 10. № 2. С. 128-133.

[2] Кибермошенничество: портрет пострадавшего // Банк России URL: https://cbr.ru/statistics/information_security/cyber_portrait/2024/ (дата обращения: 24.09.2025).

тируют внимание на использовании психологических аспектов человеческого поведения, то есть манипулировании человеческими слабостями и доверием. Они стремятся обмануть, убедить или ввести в заблуждение жертву, чтобы получить доступ к ее конфиденциальной информации такими методами.

Фишинг – рассылка обманных сообщений, маскирующихся под надежные источники, часто от имени руководства компании или службы безопасности банка. Вишинг – получение ценной информации и побуждение жертвы к определенным действиям по телефону. Захват аккаунтов электронной почты, мессенджеров и социальных сетей с последующей рассылкой сообщений от имени владельца. Часто это просьбы о финансовой помощи или ссылки на вредоносные программы. Спуфинг – создание и продвижение поддельных сайтов, имитирующих известные интернет-магазины.

Киберпреступления, несомненно, являются одним из наиболее распространенных способов проявления преступных действий в интернет-среде. Предупреждение кибервиктимного поведения в основном построено на информировании людей о различных способах мошенничества. Склонность к кибервиктимному поведению обусловлена наличием некоторых особенностей эмоционального характера и низкой осведомленностью о способах информационной преступности. Способность противостоять преступным действиям мошенников в Интернете должна базироваться на формировании у людей таких личностных особенностей, как самоконтроль эмоциональных реакций и поведения. Важна и тренировка высокой адаптации к быстро меняющейся информационной среде.

Едынак И.В.

Дальневосточный юридический институт МВД России имени И.Ф. Шилова (г. Хабаровск)

Искусственный интеллект в работе полиции: возможности и риски интеграции

Технологии искусственного интеллекта активно развиваются и внедряются абсолютно во всем в мире. На данный момент искусственный интеллект является одним из наиболее перспективных открытий в различных сферах деятельности человека. При этом в рамках применения некоторых из них, например в работе органов внутренних дел, существуют, помимо перспектив внедрения и дальнейшего развития использования, значимые риски. Применение традиционных методов борьбы с преступностью не позволяет нанести значительный ущерб результатам, чего нельзя сказать о современных технологиях. Если же безосновательно внедрять искусственный интеллект в работу полиции, то конфиденциальность используемых данных будет нахо-