УДК 343

А. С. Лаврова,
курсант 3-го курса факультета милиции
Могилевского института МВД
Н. М. Саулов,
курсант 2-го курса факультета милиции
Могилевского института МВД
Научный руководитель: Т. И. Вишневская,
начальник кафедры правовых дисциплин
факультета повышения квалификации
и переподготовки кадров
Могилевского института МВД,
кандидат юридических наук, доцент

О ПРОТИВОДЕЙСТВИИ КИБЕРКРИМИНАЛУ В РЕСПУБЛИКЕ БЕЛАРУСЬ

Современная эпоха, отмеченная цифровым прогрессом, принесла не только беспрецедентные возможности, но и новые вызовы. Республика Беларусь, интегрируясь в глобальное информационное пространство, сталкивается с ростом изощренных киберугроз, среди которых особую опасность представляют мошенничества, совершаемые с использованием информационно-телекоммуникационных технологий (далее — ИТТ).

Цифровая трансформация общества, ускоренная пандемией COVID-19 и расширением онлайн-сервисов, создала благодатную почву для злоумышленников. Социальная инженерия, подменные номера, фишинговые рассылки — эти инструменты стали оружием в руках преступников, эксплуатирующих доверчивость граждан.

В законодательстве Республики Беларусь мошенничество с использованием ИТТ трактуется как хищение имущества или приобретение права на него посредством обмана, реализованного через цифровые каналы связи — ст. 209 Уголовного кодекса Республики Беларусь (далее — УК) [1]. Специализированные составы, такие как «Компьютерное мошенничество» (ст. 212[1] УК), охватывают действия, связанные с несанкционированным доступом к данным, блокировкой систем и манипуляцией электронными платежами [1, с. 133].

Рассмотрим ключевые схемы мошенничества с использованием ИТТ, распространенные в современном киберпространстве:

− фишинг под видом государственных органов (рассылка писем от имени банков или налоговых органов с требованием «подтвердить данные» для «возврата переплаты»);

− социальная инженерия (звонки с подменой номеров, где преступники имитируют голосовые интонации сотрудников государственных органов, используют ключевые фразы, к примеру: «ваш сын попал в ДТП», «ваша банковская карта заблокирована» и др.);

− мошенничество на маркетплейсах (продажа несуществующих товаров через популярные площадки, например через Kufar.by);

− криптовалютные «пирамиды» (обещания доходности до 300 % через телеграм-каналы).

Среди инновационных методов, используемых киберпреступниками, следует выделить:

− ИИ-фишинг (нейросети, например ChatGPT, генерируют персонализированные письма, имитирующие стиль коллег или партнеров);

− дипфейк-атаки (использование поддельного голоса);

− BEC-мошенничество (атаки на корпоративные почты с целью перенаправления платежей);

− массовые звонки с помощью сим-боксов;

− криптообменники с обнуляемой историей транзакций;

− социальная инженерия для автоматизации с помощью телеграм-бота.

Опасность инновационного криминала заключается в том, что он носит организованный и транснациональный характер. Обеспечение кибербезопасности сегодня представляется архиважной задачей. Специфика современной преступности предполагает использование таких мер предупреждения, как правовые, технические, организационные. К правовым мерам предупреждения в первую очередь относятся действующие нормы законодательства. Так, в Республике Беларусь действует Указ Президента Республики Беларусь от 14 февраля 2023 г. № 40 «О кибербезопасности» [2], ежегодно вносятся изменения и дополнения в нормы уголовного законодательства. Технические средства защиты включают в себя технологическую модернизацию. К примеру, внедрение платформы «Киберщит», которая анализирует транзакции в режиме реального времени, блокируя подозрительные операции; мобильных приложений «СтопМошенник», которые позволяют гражданам проверять номера телефонов и сайты на наличие их в «черных списках», и др. Организационная защита заключается в организации деятельности по обеспечению кибербезопасности.

В заключение отметим, что криминальная сфера стремительно эволюционирует: социальная инженерия уступает место атакам с использованием искусственного интеллекта и дипфейков, а преступники все чаще действуют, находясь за пределами страны, используя анонимность криптовалют и сложности международного розыска. Поэтому можно говорить о том, что борьба с ИТ-мошенничеством в Беларуси вступила в новую, более сложную фазу.

Достигнутые правоохранительными органами результаты — от законодательных новаций и технологической модернизации до масштабной просветительской работы с населением — создали прочный фундамент. Но сама природа угрозы требует постоянного движения вперед: дальнейшего укрепления межгосударственного сотрудничества, инвестиций в криминалистические технологии, развития государственно-частного партнерства и, главное, непрерывного повышения цифровой грамотности каждого гражданина. Только такой комплексный и динамичный подход позволит эффективно защитить цифровой суверенитет страны и финансовое благополучие ее жителей в условиях постоянно меняющихся киберугроз.

1. Уголовный кодекс Республики Беларусь [Электронный ресурс] : 9 июля 1999 г. № 275-З : принят Палатой представителей 2 июня 1999 г. : одобр. Советом Респ. 24 июня 1999 г. : в ред. от 17 февр. 2025 г. № 61-З. Доступ из информ.-поисковой системы «ЭТАЛОН». Вернуться к статье

2. О кибербезопасности [Электронный ресурс] : Указ Президента Респ. Беларусь от 14 февр. 2023 г. № 40. Доступ из информ.-поисковой системы «ЭТАЛОН». Вернуться к статье