

СОЦИАЛЬНЫЕ ДЕТЕРМИНАНТЫ КИБЕРПРЕСТУПНОСТИ

Гультяева Надежда Николаевна

главный специалист отдела государственного учреждения

«Научно-практический центр проблем укрепления законности и правопорядка

Генеральной прокуратуры Республики Беларусь»

магистр юридических наук

Информационное общество предполагает возникновение глобально-го информационного пространства (цифрового пространства, киберпространства). Вместе с тем сопутствующим признаком информационного общества является и киберпреступность. Киберпреступления совершаются в информационном пространстве путем использования доступных преступникам информационных технологий. Общественная опасность киберпреступлений определяется не только национальным законодательством, но и в рамках деятельности международных организаций.

Киберриски становятся все более значимыми в деятельности финансовых организаций и потенциально могут иметь последствия для финансовой и не только финансовой стабильности целых государств, если мишенью кибератак становятся системно значимые банки, объекты государственной, финансовой инфраструктуры, включая платежные системы [1].

В Концепции национальной безопасности Республики Беларусь, утвержденной Решением Всебелорусского народного собрания от 24 апреля 2024 г. № 5, одними из основных национальных интересов в информационной сфере указаны дальнейшее развитие безопасной информационной среды и информационного общества, надежное и устойчивое функционирование национальных информационных систем и инфраструктуры, ресурсов субъектов информационных отношений, а также развитие международного информационного сотрудничества на основе национальных интересов Республики Беларусь, обеспечение сохранности государственных секретов и иной информации, распространение и (или) предоставление которой ограничено.

Принимая во внимание изложенное, предлагается определить наиболее важные социальные детерминанты киберпреступности с учетом особенностей социально-экономической ситуации, а также специфики киберпреступлений в целом: пробелы в обеспечении информационной безопасности, отсутствие эффективной защиты информационных систем; введение односторонних санкций в отношении Республики Беларусь; необходимость уточнения правового статуса криптовалют в Республике Беларусь; трансграничность киберпреступлений (невозможность установления юрисдикции, в которой находится лицо, совершившее преступление); латентность киберпреступлений (не все факты совершения противоправ-

ных действий в сети Интернет становятся известны правоохранительным органам); анонимность (невозможность установления конкретного лица (группы лиц), совершивших киберпреступления); атрибуция (перенаправление данных на другое устройство в целях сокрытия личности преступника); доступность использования новых технологий для совершения киберпреступлений; отсутствие необходимых компетенций при расследовании киберпреступлений; идеологическая составляющая; финансовые мотивы (корысть).

Рассмотрим некоторые из них.

1. Одна из основных детерминант киберпреступности – пробелы в обеспечении информационной безопасности, отсутствие эффективной защиты информационных систем, которые могут создавать уязвимости и использоваться преступниками.

В настоящее время в Республике Беларусь на законодательном уровне выстраивается надежный механизм киберзащиты. В первую очередь это связано с принятием в 2023 г. ряда нормативных правовых актов в сфере информационной безопасности: Указы Президента Республики Беларусь от 14 февраля 2023 г. № 40 «О кибербезопасности» и от 29 ноября 2023 г. № 381 «О цифровом развитии»; постановление Совета Министров Республики Беларусь от 23 февраля 2023 г. № 120 «О мерах по реализации Указа Президента Республики Беларусь от 14 февраля 2023 г. № 40»; приказ Оперативно-аналитического центра при Президенте Республики Беларусь от 25 июля 2023 г. № 130 «О мерах по реализации Указа Президента Республики Беларусь от 14 февраля 2023 г. № 40».

Отметим также Указ Президента Республики Беларусь от 29 августа 2023 г. № 269 «О мерах по противодействию несанкционированным платежным операциям», благодаря которому удалось изменить ситуацию с хищениями со счетов граждан. Так, по итогам первых четырех месяцев 2023 г. было зарегистрировано 5 тыс. краж со счетов граждан, а за аналогичный период 2024 г. таких преступлений зафиксировано чуть больше 2 тыс. [2].

2. Введение односторонних санкций в сфере финансовых технологий.

В настоящее время пробелы в обеспечении информационной безопасности, отсутствие эффективной защиты информационных систем связаны в том числе с введением односторонних санкций странами ЕС и США в отношении Республики Беларусь в финансовом секторе, в том числе в секторе финансовых технологий (*FinTech*) [3]. Финтех генерирует и множественные киберриски, связанные с кибератаками, использованием небанковских участников в так называемых «серых схемах» отмывания денег, мошеннических переводах, а также финансировании деструктивной деятельности, включая терроризм [4].

Самыми болезненными потерями практики называют операционные решения в сфере мониторинга, фильтрации и блокировки атак на веб-

приложения. В Российской Федерации, да и в Республике Беларусь, все системы информационной защиты построены на иностранном ядре Linux, которое никто заново не перепишет. Тот же Linux писался мировым сообществом, – отмечают специалисты. Можно заменить иностранные ветки репозитивов (уязвимостей), чтобы через обновления нельзя было скачать закладки хакеров, но все заменить невозможно. Можно использовать только компенсационные меры. Многие организации, в том числе финансовые, начали замещать всю кибербезопасность с начала 2020 г. [5].

Новыми точками роста для белорусского финтех в условиях международных санкций может стать разработка альтернативных инструментов для международных переводов со странами – участниками ЕАЭС, Китаем, Индией, ОАЭ, Латинской Америкой, Африкой.

3. Необходимость уточнения правового статуса криптовалют в Республике Беларусь.

Криптовалюты, такие как биткойн, обладают анонимностью и псевдоанонимностью, что делает их привлекательным средством для совершения преступлений в сети. За счет сложности отслеживания операций с криптовалютой, злоумышленники могут оставаться в тени, усложняя задачу правоохранным органам. Появление ресурсов по обмену криптовалютой без гарантии стимулирует киберпреступность, создавая новые возможности для криминальной деятельности в цифровой среде.

Республика Беларусь одной из первых стран в мире признала законной работу с криптовалютами. Согласно положениям Декрета Президента Республики Беларусь от 21 декабря 2017 г. № 8 «О развитии цифровой экономики» физические лица на территории Республики Беларусь вправе владеть токенами и с учетом особенностей, установленных национальным законодательством, совершать следующие операции: майнинг, хранение токенов в виртуальных кошельках, обмен токенов на иные токены, их приобретение, отчуждение за белорусские рубли, иностранную валюту, электронные деньги, а также дарить и завещать токены.

Правовой статус криптовалют в Республике Беларусь определяется рядом нормативных правовых актов. Это прежде всего Декрет Президента Республики Беларусь от 21 декабря 2017 г. № 8 «О развитии цифровой экономики», Указ Президента Республики Беларусь от 17 сентября 2024 г. № 367 «Об обращении цифровых знаков (токенов)».

Для регулирования оборота криптовалют, как на внутреннем рынке Республики Беларусь, так и на внешнем, недостаточно понятийного аппарата, предусмотренного в приложении 1 к Декрету № 8.

Так, определение термина «размещение цифровых знаков (токенов)», которое предполагает совершение гражданско-правовых сделок либо иных юридически значимых действий, направленных на передачу цифровых знаков (токенов) их первым владельцам на условиях, определенных лицом, со-

здавшим через резидента Парка высоких технологий такие цифровые знаки (токены), в том числе в целях привлечения от первых владельцев белорусских рублей, иностранной валюты, электронных денег, цифровых знаков (токенов) другого вида, не охватывает в полной мере все сделки, совершаемые с криптовалютами на внутреннем и внешнем рынке цифровых знаков.

По мнению автора, стоит провести сравнительную характеристику Закона № 226-З с нормативными правовыми актами, регулирующими вопросы обращения криптовалют, и рассмотреть возможность введения в законодательство Республики Беларусь таких правовых терминов и их определений как «криптовалютные операции» или «операции с токенами», «крипто-обменные операции», «криптовалютный договор», «внутренний криптовалютный рынок», «иностранный оператор криптовалютной платформы», «иностранный оператор обмена криптовалют».

Список цитированных источников

1. Федорова, И. А. Киберпреступность в сфере финансовых технологий [Электронный ресурс]: [по состоянию на 25.05.2024 г.] / И. А. Федорова, А. И. Яговкина // КонсультантПлюс. Россия / ЗАО «Консультант Плюс». – М., 2024.
2. «В тренде уже не хищение денег». В МВД рассказали об изменении структуры киберпреступности [Электронный ресурс]. – Режим доступа: <https://www.pravo.by/novosti/obshchestvenno-politicheskie-i-v-oblasti-prava/2024/maj/77745/> – Дата доступа: 25.05.2024.
3. Санкции в отношении Беларуси [Электронный ресурс]. – Режим доступа: <https://belarus.ahk.de/ru/infoteka/sankcii-v-otnoshenii-belarusi>. – Дата доступа: 01.03.2024.
4. Дорошенко, И. А. Развитие финтех-индустрии в Российской Федерации в условиях международных санкций [Электронный ресурс] / И. А. Дорошенко // Финансы. Налогообложение. Кредит. – 2022. – С. 35–41. – Режим доступа: <https://cyberleninka.ru/article/n/razvitiye-finteh-industrii-v-rossiyskoy-federatsii-v-usloviyah-mezhdunarodnyh-sanktsiy/viewer>. – Дата доступа: 05.06.2024.
5. Герасимов, А. Как финтех оценивает киберриски в условиях санкций [Электронный ресурс] / А. Герасимов // Securitylab.ru. – 2022. – Режим доступа: <https://www.securitylab.ru/blog/company/awillix/352283.php>. – Дата доступа: 24.05.2024.

ИСПОЛЬЗОВАНИЕ БЕСПИЛОТНЫХ ЛЕТАТЕЛЬНЫХ АППАРАТОВ ПРИ СОВЕРШЕНИИ УМЫШЛЕННЫХ ПРЕСТУПЛЕНИЙ: ПУТИ КРИМИНАЛИЗАЦИИ

Дрозд Александра Николаевна

*доцент кафедры уголовного права учреждения образования
«Академия Министерства внутренних дел Республики Беларусь»,
кандидат юридических наук
drozd-amvd@yandex.by*

Выступая на совещании с руководящим составом государственных органов системы обеспечения национальной безопасности в феврале нынешнего года, Президент Республики Беларусь Александр Григорьевич