УДК 343.3/.7 DOI: 10.17277/pravo.2026.01.pp.108-114

КИБЕРПРЕСТУПНОСТЬ В СОВРЕМЕННОМ МИРЕ: ЦИФРОВИЗАЦИЯ И ЕЕ ВЫЗОВЫ УГОЛОВНОМУ ПРАВУ

Эдуард Николаевич Лыков, *канд. филос. наук, доцент, кафедра юридических дисциплин, филиал ФГАОУ ВО «Российский государственный гуманитарный университет» в г. Домодедово Московской области, Домодедово, Россия; likedik@mail.ru*

Алексей Иванович Бельский, *канд. юрид. наук, доцент, начальник кафедры уголовного процесса, ФГКОУ ВО «Белгородский юридический институт МВД России имени И. Д. Путилина», Белгород, Россия; sembel77@yandex.ru*

На сегодняшний день человечество становится свидетелем самой масштабной цифровизации, которая затрагивает практически все сферы жизнедеятельности людей. На постоянной основе используются новые технологии, которые, бесспорно, облегчают жизнь человека, но вместе с тем становятся источниками повышенной опасности и ставят под угрозу нормальное течение общественной жизни. С помощью цифровых технологий у злоумышленников появляется все больше и больше возможностей для совершения преступлений, и при этом остаться незамеченными. Предложены к рассмотрению современные виды киберпреступлений, а также проведен анализ актуальных проблем их квалификации и способов противодействия на основании норм действующего законодательства. Особое внимание обращено на пробелы в законодательстве и возможные пути его совершенствования в условиях стремительного развития и использования цифровых технологий.

Ключевые слова: информационная безопасность; информация; квалификация преступлений; кибермошенничество; киберпреступность; мошенники; преступник.

Введение

В современном мире цифровые технологии стали неотъемлемой частью жизни каждого человека. Активная цифровизация предполагает, что вся информация, которая касается жизни человека, должна быть перенесена с бумажных носителей в виртуальное пространство. Это происходит в целях упрощения пользования информацией, рациональному использованию человеческого и материального ресурса. Но вместе с тем преступная деятельность перемещается в виртуальное пространство, изобретая все новые и новые способы использования информации в корыстных целях, принося людям материальный и моральный ущерб, а также ставя под сомнение всю систему информационной безопасности. С каждым разом киберпреступность приобретает все новые и новые формы, тем самым усложняет процесс ее противодействию [1]. Существующие нормы уголовного законодательства не успевают адаптироваться к новым формам киберпреступности, из-за чего преступники продолжают находиться на шаг

впереди. Различные способы мошенничества, которые совершаются с использованием цифровых технологий могут создавать ущерб разного масштаба, начиная с посягательства на личность и заканчивая атаками на критическую инфраструктуру. Кроме того, цифровые технологии стали популярны в использовании преступниками криптовалютных схем с целью отмывания денег. Все перечисленные виды преступлений с использованием цифровых технологий заставляют переосмыслить используемые уголовно-правовые механизмы противодействия.

Обсуждение

На современном этапе развития цифровых технологий существуют следующие *виды киберугроз*.

Фишинг и социальная инженерия. В последние годы проявление фишинга имеет самый массовый характер. Преступник выбирает способ войти в доверие к потенциальной жертве, притворившись его близким человеком или представителем какой-либо организации и учреждения (сотрудником МВД или банка, или мобильного оператора и т.д.). После того, как преступник установил контакт с жертвой, он производит рассылку поддельных писем или SMS-сообщений в мессенджерах. Данные виды киберугроз особенно опасны тем, что используют человеческую доверчивость, а мошенники играют на чувствах людей, при этом техническая уязвимость исполняет в данном случае не первостепенную роль. Преступник ждет от своей жертвы следующих действий:

– переход на фальшивый сайт и ввод личных данных;

– установки на свой персональный компьютер или смартфон вредоносного программного обеспечения;

– перевод денежных средств или оплата какого-либо платежа на счет мошенников [3].

В качестве наглядного примера фишинга может служить ситуация, когда потенциальной жертве поступило письмо из банка, в котором отражена просьба актуализировать паспортные данные для входа в личный кабинет. В сообщении содержится ссылка, по которой необходимо перейти и ввести необходимые данные.

Также следует обратить внимание на понятие «социальная инженерия», что подразумевает собой манипулирование людьми с целью получения личной информации или доступа к различным системам без помощи технических уязвимостей. Социальная инженерия включает в себя следующие методы:

– «протекстинг» – создание несуществующего сценария (звонок из коммунальной службы или органов внутренних дел);

– «квипрокво» (от лат. *qui pro quo*) – предложение установить вредоносную программу под видом обновления текущего программного обеспечения;

– «троянский конь» – преступник выдает себя сотрудником различных компаний или ведомств, тем самым сразу входит в доверие и настойчиво требует данные от жертвы.

Все это позволяет преступнику получить полный контроль над личными данными жертвы и использовать их в преступных целях. На сегодняшний день в России фишинг и социальная инженерия попадают под уголовную ответственность в рамках ст.ст. 159, 272, 273 УК РФ. Наказание за подобные виды преступлений начинается от назначения денежного штрафа и заканчивается лишением свободы на срок до 10 лет в зависимости от тяжести совершенного деяния [4].

Атаки на критическую инфраструктуру. Кроме посягательства на личность, мошенники не раз осмеливаются предпринимать атаки на государственные информационные системы, банки и объекты энергетики, что может повлечь за собой масштабный и непоправимый ущерб для большого числа людей. Данный вид преступлений квалифицируется по ст. 274.1 УК РФ (неправомерное воздействие на критическую информационную инфраструктуру). Преступник целенаправленно воздействует с помощью цифровых технологий на системы, которые напрямую обеспечивают деятельность жизненно важных объектов (электростанции и электросети, транспортная инфраструктура, финансовые системы, органы и учреждения здравоохранения, системы водоснабжения, телекоммуникации) [6]. Цели преступного посягательства на объекты критической инфраструктуры могут быть различными, например:

– дестабилизация ситуации в стране;

– шантаж и вымогательство;

– оказание политического давления;

– диверсии или подготовка к реальным боевым действиям.

В качестве примеров следует вспомнить атаку под названием BlackEnergy на Украине, когда в 2015 году произошла кибератака и массовое отключение электричества по всей стране, а также события 2021 года в США, когда произошла парализация топливного трубопровода. Из-за своего масштаба такой вид преступного посягательства требует международного и междисциплинарного взаимодействия для разработки наиболее эффективных методов противодействия таким угрозам [2].

Использование криптовалют в преступных целях. Главной проблемой эффективного противодействия данному виду преступлений (ст. 174 УК РФ) является отсутствие слаженного международного сотрудничества по урегулированию вопроса существования и использования криптовалют, а также невозможность точного и последовательного отражения транзакций. Криптовалюта так популярна у преступников по нескольким причинам: глобальная доступность, децентрализация и псевдоанонимность. Одними из самых популярных преступлений и использованием криптовалют являются:

– отмывание денег, сюда входят несколько способов, при помощи которых преступники производят отмывание денег:

а) смешивание – при помощи вспомогательных сервисов происходит перетасовка транзакций для сокрытия первоначального источника средств (Blender.io, TornadoCash);

б) цепочка обменов – злоумышленниками производится перевод через несколько блокчейнов и обменников (например, по схеме Bitcoin–Monero–Ethereum);

в) крипто-фиатные схемы, при помощи которых происходит обналичивание денежных средств, при этом могут принимать участие OTC-брокеры и подставные компании;

– теневые рынки (Darknet), при помощи которых происходит покупка или продажа запрещенных предметов и веществ (оружия, наркотиков, поддельных документов), а также происходит оплата услуг хакеров и торговля запрещенного контента (детская эксплуатация);

– киберпреступления, сюда включен следующий перечень запрещенных деяний:

а) Ransomware-атаки, при которых мошенники просят выкуп в той или иной криптовалюте;

б) фишинговые схемы, которые предполагают использование несуществующих интернет-кошельков;

в) криптодженкинг – майнинг на зараженных устройствах;

– уклонение от санкций, данный вид нарушений используется при обходе банковских ограничений, которые, например, возникли после событий 2022 года и введения массовых санкций. Кроме того, сюда попадают и незаконные международные переводы (Иран, КНДР, РФ) [7].

Киберклевета и deepfake. В условиях стремительного внедрения использования искусственного интеллекта в жизнь человека злоумышленники нашли способ создавать поддельные аудио- и видеоматериалы, которые впоследствии используются с целью обмана или шантажа потенциальной жертвы. С помощью deepfake создаются видео с участием известных политиков и знаменитостей, директоров крупных компаний, которые используются мошенниками с масштабным целями, такими как дестабилизация обстановки в обществе или крупное финансовое хищение. Также с помощью данной технологии проводятся политические провокации, например, в Индии в 2024 году при помощи дипфейк-видеоролика с участием кандидата в депутаты разожглись массовые общественные волнения.

С точки зрения действующего уголовного законодательства, такие действия преступника попадают под ст. 128.1 (клевета) или ст. 138 УК РФ (нарушение тайны частной жизни). Что касается подделки аудио- и видеоматериалов, так называемого deepfake, то законодательство пока не учитывает такую специфику преступлений из-за существующего пробела в нем.

Киберпреступления создают множество проблем при квалификации данного вида преступлений. Главной сложностью выступает наличие следующих факторов:

– транснациональность, которая позволяет преступникам действовать абсолютно из любой точки мира, что значительным образом затягивает процесс расследования преступления или делает это вовсе невозможным;

– анонимность, данную проблему усугубляет использование таких сервисов, как VPN, TOR и криптовалют, значительным образом усложняет процесс идентификации личности преступника, не говоря уже о поисках его местонахождения;

– совершенствование методов и их непрерывная изменчивость, что не позволяет законодательству адаптироваться под новые методы совершения преступлений с использованием цифровых технологий;

– недостаточная техническая оснащенность подразделений правоохранительных органов, которые занимаются противодействием данного вида преступлениям. Кроме того, проблему создает недостаточная профильная подготовленность кадров, которые не имеют должного уровня теоретической и практической подготовки, позволяющей эффективно бороться с киберпреступниками [5].

Заключение

Таким образом, для того чтобы повысить эффективность борьбы с киберпреступностью в современных условиях развития цифровизации, необходимо внести ряд следующих изменений и дополнений в УК РФ.

1. Расширить и детализировать следующие составы преступлений:

а) ужесточить наказание за совершение преступлений, предусмотренных ст. 272 УК РФ, а именно за взлом критической инфраструктуры, которые включают в себя посягательства на банки, государственные учреждения, ЖКХ и т. д.;

б) ввести дифференцированную ответственность в зависимости от масштаба нанесенного ущерба за использование программ-шифровальщиков и DDoS-атак, при совершении преступлений, предусмотренных ст. 273 УК РФ, которая запрещает создание, использование и распространение вредоносных программ;

в) распространить действие ст. 274 УК РФ на облачные сервисы и криптоплатформы.

2. Ввести в УК РФ статьи, которые предусматривают ответственность за следующие деяния:

а) кибермошенничество в его различных проявлениях (фишинг, кардинг и социальная инженерия), где для каждого отдельного вида кибермошенничества будет предусмотрена дифференцированная ответственность в зависимости от тяжести нанесенного ущерба;

б) кибертерроризм (атаки на системы жизнеобеспечения страны и угрозы национальной безопасности);

в) незаконный оборот цифровых активов, то есть отмывание денежных средств при помощи криптовалют и использования Darknet.

3. Ужесточить ответственность для IT-специалистов за преднамеренное оказание помощи кибермошенникам (создание вредоносного программного обеспечения). Следует ужесточить наказание для IT-специалистов, работающих на предприятиях и отвечающих за защиту информации и баз данных, так как утечки информации зачастую происходят из-за халатности сотрудников.

Все вышеуказанные предложения позволят значительно снизить количество киберпреступлений и осуществить эффективную борьбу с новыми ее проявлениями. Необходимо непрерывно и тщательно следить за возможными способами совершения преступлений с использованием информационных технологий, для того чтобы своевременно вносить изменения в действующее законодательство и предотвращать возможности массовых атак злоумышленников.

Список литературы

1. Бондарев, В. В. Введение в информационную безопасность автоматизированных систем : учебное пособие / В. В. Бондарев. – Москва : Изд-во МГТУ им. Н. Э. Баумана, 2024. – 252 с.

2. Дубень, А. К. Международное сотрудничество в сфере информационной безопасности: общая характеристика и российский подход к изучению / А. К. Дубень // Международное право и международные организации. – 2022. – № 1. – С. 24–33. doi: 10.7256/2454-0633.2022.1.37490

3. Жарова, А. К. Защита информации ограниченного доступа, получаемой по цифровым каналам передачи информации о совершаемых коррупционных правонарушениях / А. К. Жарова // Государственная власть и местное самоуправление. – 2023. – № 9. – С. 37–41. doi: 10.18572/1813-1247-2023-9-37-41

4. Зенков, А. В. Информационная безопасность и защита информации / А. В. Зенков. – Москва : Юрайт, 2023. – 108 с.

5. Росиков, А. Защита конфиденциальной информации / А. Росиков // Юридический справочник руководителя. – 2023. – № 8. – С. 25–37. – URL : https://трудовые-договоры.рф/article/1799 (дата обращения: 26.01.2026).

6. Хорев, П. Б. Программно-аппаратная защита информации : учебное пособие / П. Б. Хорев. – Москва : ИНФРА-М, 2022. – 327 с.

7. Щербак, А. В. Информационная безопасность : учебник для вузов / А. В. Щербак.– 2-е изд. – Москва : Юрайт, 2023. – 260 с.

References

1. Bondarev V.V. *Vvedeniye v informatsionnuyu bezopasnost' avtomatizirovannykh sistem: uchebnoye posobiye* [Introduction to Information Security of Automated Systems: a textbook], Moscow: Izdatel'stvo MGTU im. N.E. Baumana, 2024, 252 p. (In Russ.)

2. Duben' A.K. [International cooperation in the field of information security: general characteristics and the Russian approach to the study], *Mezhdunarodnoye pravo i mezhdunarodnyye organizatsii* [International law and international organizations], 2022, no. 1, pp. 24-33. doi: 10.7256/2454-0633.2022.1.37490 (In Russ., abstract in Eng.)

3. Zharova A. K. [Protection of restricted information received via digital channels for transmitting information on corruption offenses], *Gosudarstvennaya vlast' i mestnoye samoupravleniye* [State power and local self-government], 2023, no. 9, pp. 37-41. doi: 10.18572/1813-1247-2023-9-37-41 (In Russ., abstract in Eng.)

4. Zenkov A.V. *Informatsionnaya bezopasnost' i zashchita informatsii* [Information Security and Information Protection], Moscow: Yurayt, 2023, 108 p. (In Russ.)

5. Rosikov A. [Protection of Confidential Information], *Yuridicheskiy spravochnik rukovoditelya* [Legal Handbook of the Manager], 2023, no. 8, pp. 25-37, available at: https://trudovyye-dogovory.rf/article/1799 (accessed 26 January 2026).

6. Khorev P.B. *Programmno-apparatnaya zashchita informatsii: uchebnoye posobiye* [Software and Hardware Information Protection: A Study Guide], Moscow: INFRA-M, 2022, 327 p. (In Russ.)

7. Shcherbak A.V. *Informatsionnaya bezopasnost': uchebnik dlya vuzov* [Information Security], Moscow: Yurayt, 2023, 260 p. (In Russ.)

Cybercrime in the Modern World: Digitalization and its Challenges to Criminal Law

E. N. Lykov, *Cand. Sci. (Philosophy), Associate Professor, Department of Legal Disciplines, Branch of the Russian State University for the Humanities in Domodedovo, Moscow Region, Domodedovo, Russia; likedik@mail.ru*

A. I. Belsky, *Cand. Sci. (Law), Associate Professor, Department of Criminal Law Disciplines, Belgorod Law Institute of Ministry of the Interior of the Russian Federation named after I. D. Putilin, Belgorod, Russia; sembel77@yandex.ru*

Today, the world is witnessing the most extensive digitalization, affecting virtually every aspect of human life. New technologies are constantly being used, undoubtedly making human life easier, but at the same time, they are becoming sources of increased danger and threatening the normal functioning of society. Digital technologies provide criminals with ever-increasing opportunities to commit crimes while remaining undetected. This article presents a review of modern types of cybercrime, as well as an analysis of current issues in their classification and methods of combating them based on current legislation. Particular attention is paid to gaps in legislation and possible ways to improve it in the context of the rapid development and use of digital technologies.

Keywords: information security; information; crime classification; cyber fraud; cybercrime; scammers; criminal.

Статья поступила в редакцию 18.09.2025

При цитировании использовать:

Лыков Э. Н., Бельский А. И. Киберпреступность в современном мире: цифровизация и ее вызовы уголовному праву // Право: история и современность. – 2026. – Т. 10, № 1. – С. 108 – 114. doi: 10.17277/pravo.2026.01.pp.108-114