

стороны осужденных; необходимости баланса между официальной дистанцией и установлением профессионального контакта для получения информации; внутренней служебной коммуникации, требующей четкости, субординации и оперативности.

Для повышения коммуникативной компетентности и культуры общения необходимо заниматься с сотрудниками, осуществлять дополнительную профессиональную подготовку в данном направлении. При этом выявляются трудности, связанные с преобладанием теоретического обучения над практическими формами, недостаточного внимания к отработке навыков распознавания и парирования манипуляций, слабая интеграция психологического блока с правовыми и специальными дисциплинами.

В настоящий момент оптимизация требует внедрения сквозного модуля «Профессиональная коммуникация в УИС», объединяющего юридические, психологические и служебные аспекты. Необходимо увеличить долю интерактивных методов, таких как тренинги ролевого общения, анализ видео-кейсов, симуляции критических ситуаций и многое другое¹. Следует разработать дифференцированные коммуникативные программы для различных категорий сотрудников, создать системы со-

провождения молодых специалистов, где более опытные сотрудники оказывают помощь при разрешении сложных коммуникативных случаев из практики. Особое внимание следует обратить на применение VR-тренажеров для отработки действий и коммуникации в смоделированных стрессовых ситуациях, развитию этических норм, проведения регулярных брифингов по обмену коммуникативным опытом, использовать поощрение конструктивного стиля взаимодействия. Психологическим службам необходимо регулярно проводить тренинги по профилактике эмоционального выгорания, которое напрямую снижает коммуникативную эффективность.

Оптимизация коммуникативной компетентности сотрудников УИС является главной задачей, от решения которой зависят безопасность и гуманизация пенитенциарной системы. Для достижения качественно нового уровня необходим переход от фрагментарного обучения к системной психолого-ориентированной модели подготовки, где коммуникация является основным инструментом служебной деятельности. Реализация предложенных мер будет способствовать формированию у сотрудников устойчивых навыков эффективного и профессионального общения, повышая общую эффективность работы учреждений УИС.

Овсянников П.Ю.,

кандидат юридических наук

Сибирский юридический институт МВД России (г. Красноярск)

Институты гражданского права как инструменты противодействия преступлениям в цифровой среде

В эпоху цифровизации преступления в цифровой среде стали одной из наиболее острых проблем современно-

го общества. Под «цифровыми преступлениями» в широком смысле понимаются как уголовно наказуемые деяния

¹ Баранов А.М. Активные методы обучения в профессиональной подготовке сотрудников правоохранительных органов: теория и практика. М. : ЮНИТИ-ДАНА, 2019. 215 с.

(кибермошенничество, хакерские атаки, распространение вредоносного программного обеспечения), так и правонарушения, не влекущие уголовной ответственности, но причиняющие вред имущественным и личным неимущественным благам граждан и организаций. В то время как уголовно-правовые меры остаются ключевым элементом репрессивной политики, все большую роль начинают играть гражданско-правовые инструменты, направленные на восстановление нарушенных прав, предотвращение ущерба и стимулирование добросовестного поведения участников цифрового оборота.

Цифровые преступления характеризуются высокой латентностью, трансграничностью, анонимностью и технической сложностью. Они могут затрагивать:

право собственности (хищение цифровых активов, криптовалют);

неприкосновенность частной жизни и защиту персональных данных;

деловую репутацию (распространение ложной информации в сети);

авторские и смежные права (пиратство, нелегальное копирование контента);

корпоративные интересы (утечка коммерческой тайны, DDoS-атаки¹).

Стоит отметить, что не каждое такое противоправное деяние квалифицируется как преступление. Некоторые из них являются предметом гражданско-правовой охраны и влекут наступление гражданско-правовой ответственности.

Рассмотрим основные гражданско-правовые институты, направленные на противодействие преступлениям в цифровой среде.

Одним из фундаментальных институтов гражданско-правовой защиты являются иски о компенсации ущерба,

причиненного цифровыми преступлениями. В цифровой среде ущерб может быть материальным (финансовые потери от мошенничества) или нематериальным (моральный вред от утечки данных или клеветы).

В соответствии со статьей 1064 Гражданского кодекса Российской Федерации вред, причиненный личности или имуществу гражданина, подлежит возмещению в полном объеме лицом, причинившим вред. В цифровой среде это применимо, например:

при утечке персональных данных вследствие ненадлежащей защиты со стороны оператора;

при распространении порочащих честь, достоинство и деловую репутацию сведений в информационно-телекоммуникационной сети Интернет (статья 152 ГК РФ);

при неправомерном использовании программного обеспечения или цифрового контента.

Судебная практика все чаще признает вред, причиненный в цифровой среде, подлежащим компенсации, включая моральный вред.

Некоторые цифровые преступления связаны с мошенничеством при заключении онлайн-сделок (например, фишинг², подмена реквизитов). В таких случаях потерпевший может обратиться в суд с требованием о признании сделки недействительной на основании статей 166-181 ГК РФ, но для этого нужно доказать обман или злоупотребление доверием.

Главой 70 ГК РФ предусмотрен широкий перечень средств защиты авторских и смежных прав в цифровой среде: требование о прекращении нарушения;

изъятие контрафактных копий;

1 DDoS-атака – это массовая и целенаправленная отправка запросов на сервер с целью перегрузить его и сделать недоступным для пользователей.

2 Фишинг – вид интернет-мошенничества, при котором злоумышленники пытаются выманить конфиденциальные сведения: логины, пароли, реквизиты банковской карты, доступы к корпоративным сервисам.

возмещение убытков или выплата компенсации (в том числе в виде двукратной стоимости незаконно использованного контента¹).

Поставщики цифровых услуг обязаны реагировать на уведомления правообладателей о нарушении авторских и смежных прав (механизм «notice-and-takedown»²), что также является гражданско-правовым инструментом, хотя и реализуется через договорные отношения.

С развитием искусственного интеллекта и автоматизированных систем возникает вопрос ответственности за вред, причиненный их функционированием. Несмотря на то что законодательство в этой сфере еще в процессе формирования, уже сейчас применяются конструкции риска деятельности таких информационных систем (статья 1079 ГК РФ): владелец источника повышенной опасности (включая сложные ИТ-системы) несет ответственность независимо от вины.

Особое место среди рассматриваемых институтов занимает договорно-правовое регулирование. Гражданское право позволяет сторонам заранее распределить риски цифровых угроз через договор:

соглашение о неразглашении конфиденциальных сведений (NDA³);

пользовательское соглашение с условиями обработки данных и ответственности за нарушение;

соглашение с поставщиками цифровых услуг, предусматривающие ответственность за нарушения в защите данных (Service Level Agreement⁴).

Такие соглашения учитываются судами при разрешении споров, возникающих в цифровой среде.

Несмотря на наличие указанных выше гражданско-правовых институтов, направленных за защиту нарушенных прав, правовая защита в цифровой среде сталкивается с такими вызовами, как трудности установления личности правонарушителя, отсутствие четких критериев определения размера вреда (особенно морального), пробелы в правовом регулировании новых цифровых объектов (NFT⁵, децентрализованные приложения, метавселенные), юрисдикционные проблемы в трансграничных случаях.

Представляется, что перспективы развития гражданского законодательства будут связаны с правовым регулированием цифровых прав и цифровых активов, а также внедрением механизмов цифровой идентификации и блокчейн-аудита для фиксации фактов нарушений.

Гражданско-правовые институты представляют собой гибкий и проактивный подход в борьбе с преступлениями в цифровой среде. Они не заменяют уголовно-правовые меры, а играют дополняющую и превентивную роль в борьбе с преступлениями в цифровой среде. Их преимущество заключается в гибкости, ориентация на восстановление нарушенного права и возможность применения даже при отсутствии состава преступления. В условиях стремительной цифровизации общества развитие гражданско-правовых механизмов защиты становится не просто необходимым, но и стратегически важным направлением правовой политики Российской Федерации.

1 Решение Арбитражного суда Кабардино-Балкарской Республики от 28.12.2017 № А20-3517/2015.

2 С англ. Notice-and-takedown – термин, который означает процедуру уведомления и удаления контента в информационно-телекоммуникационной сети Интернет.

3 NDA (с англ. non-disclosure agreement) – соглашение о неразглашении конфиденциальной информации.

4 SLA (с англ. Service Level Agreement) – соглашение об уровне сервиса.

5 NFT (с англ. non-fungible tokens) – разновидность криптографических токенов, каждый экземпляр которых уникален и не может быть заменен другим аналогичным токеном.