УДК 342

ИНСТИТУТ ЦИФРОВОГО ОБЫСКА В РЕСПУБЛИКЕ БЕЛАРУСЬ СКВОЗЬ ПРИЗМУ ПРЕЦЕДЕНТНОЙ ПРАКТИКИ ЕВРОПЕЙСКОГО СУДА ПО ПРАВАМ ЧЕЛОВЕКА

С. С. ПЕТРОВСКАЯ
(Представлено: канд. юрид. наук, доц. И. В. Шахновская)

В статье анализируется проблема правового регулирования «цифрового обыска» и дистанционного доступа к компьютерной информации в уголовном процессе Республики Беларусь. Автор обосновывает, что действующая статья 204[1] УПК не учитывает специфику облачных хранилищ и систем «умного дома», снижая уровень процессуальных гарантий при выгрузке данных вне места следственного действия. На основе анализа прецедентной практики Европейского Суда по правам человека доказано, что объем вмешательства в частную жизнь должен определять строгость процедур, независимо от физического или цифрового формата носителя.

Включение в Уголовно-процессуальный кодекс Республики Беларусь (далее – УПК) Республики Беларусь статьи 204[1] («Осмотр компьютерной информации») является реакцией законодателя на внедрение и использование различных цифровых технологий в различных сферах, однако правоприменительная практика и доктрина столкнулись с феноменом цифрового (дистанционного) обыска, известного как отдельный институт уголовно-процессуального права в зарубежных государствах. Так, понятие цифрового (дистанционного) обыска можно определить как принудительное получение компьютерной информации, связанной с конкретным жилищем либо с частной жизнью проживающих в нём лиц, без входа в это жилище и без исследования носителя, изъятого на месте. УПК отдельного состава такого действия не предусматривает: обыск и выемка регулируются статьями 208–210 УПК, а осмотр компьютерной информации – статьёй 204[1] УПК [1]. При этом осмотр компьютерной информации проводится на месте следственного действия; если доступ к ней осуществляется посредством аутентификации пользователя либо она содержит информацию о частной жизни, сведения, составляющие охраняемую законом тайну, или иную информацию, распространение и предоставление которой ограничено, требуется согласие обладателя информации или санкция прокурора, а в неотложном случае – направление прокурору сообщения в течение 24 часов [1]. Аналогичный подход закреплён и для осмотра жилища: согласно части 7 статьи 204 УПК он проводится только с согласия собственника или проживающих в нём совершеннолетних лиц либо по постановлению следователя, органа дознания с санкции прокурора или его заместителя [1]. Санкция прокурора на обыск, осмотр жилища и осмотр компьютерной информации предусмотрена также пунктом 14 части 5 статьи 34 и частью 5 статьи 38 УПК [1].

Проблема состоит в том, что статья 204[1] УПК не рассчитана на облачные хранилища и внешние видеорегистраторы, поскольку они часто находятся не «на месте» производства следственного действия [1]. В результате при изъятии устройства в квартире действуют статьи 204 и 208–210 УПК, а при выгрузке того же архива у оператора применяется более мягкий режим статьи 204[1] УПК, в том числе по части 5 этой статьи [1]. Наименование действия меняется, но объём вторжения в частную жизнь остаётся тем же. Иными словами, уровень правовой защиты начинает зависеть от юридической квалификации действия, а не от того, какая часть домашней жизни фактически раскрыта.

Понятие жилища, закреплённое в пункте 6 статьи 6 УПК [1], остаётся пространственным: оно охватывает помещение, предназначенное для постоянного или временного проживания людей, а также его составные части, используемые для отдыха, хранения имущества либо удовлетворения иных потребностей человека, но не включает облачные хранилища и видеорегистраторы, расположенные вне квартиры. Этот вывод согласуется и с Жилищным кодексом, который такие объекты жилищем не признаёт. Вместе с тем «умный дом» создаёт цифровой контур того же пространства, которое статьи 13 и 14 УПК охраняют как частную жизнь и неприкосновенность жилища. Поэтому формальное несовпадение физического и цифрового контура жилища не должно автоматически снижать уровень гарантий.

Специальное регулирование разрыв не закрывает. Ни один из действующих актов не выравнивает гарантии дистанционного доступа к домашнему архиву с гарантиями осмотра и обыска жилища. Пока это так, контроль зависит от того, как назвали действие, а не от того, какая часть частной жизни раскрыта.

В данном направлении весьма полезна для исследования судебная практика Европейского Суда по правам человека (далее – Суд).

К примеру, показательна позиция Суда в постановлении по делу Särgava v. Estonia («Сяргава против Эстонии»). В жилище и в автомобиле адвоката были изъяты ноутбук и телефон, после чего массив данных просматривался по ключевым словам, избранным самим органом расследования. Санкция на обыск имелась. Нарушение статьи 8 Конвенции о защите прав человека и основных свобод [2]. Суд тем не менее

установил: национальный закон не определял порядок отделения относящихся к делу сведений от избыточных и не закреплял, кто этот отбор контролирует [3]. На наш взгляд, применительно к облачному архиву квартирной камеры тот же риск проявляется ещё явственнее. Физический носитель в жилище может отсутствовать, тогда как объём сведений, доступных по одному запросу, способен охватить домашнюю жизнь за значительный период.

К той же мысли Суд вернулся в постановлении по делу Podchasov v. Russia («Подчасов против России»). Нарушением было признано уже не единичное следственное действие в жилище, а общее законодательное правило, допускавшее хранение содержания интернет-коммуникаций и их передачу властям при отсутствии надлежащих ограничений [4]. На наш взгляд, значение этого вывода для систем «умного дома» состоит в следующем. Требование передать «все записи камеры, установленной в квартире» по характеру вмешательства ближе к сплошному снятию переписки, нежели к осмотру конкретного предмета.

Наконец, в постановлении по делу Černý and Others v. the Czech Republic («Черны и другие против Чехии») смартфон и планшет были изъяты при обыске жилища, а переписка с защитниками оказалась в материалах уголовного дела. Суд указал, что наличия разрешения на обыск недостаточно: порядок обращения с данными электронных устройств должен быть урегулирован отдельно, с тем чтобы исключить попадание в дело сведений, выходящих за пределы цели следственного действия [5]. На наш взгляд, если такие требования предъявляются к носителю, уже находящемуся в распоряжении органа уголовного преследования, тем более они необходимы при дистанционном получении тех же сведений без ведома проживающего.

На основании вышеизложенного, можно сформулировать следующие требования к порядку проведения обыска в жилище, связанным с изъятием цифровых технологий:

1. Получение сведений, фиксирующих домашнюю (частную) жизнь, образует вмешательство и при отсутствии вхождения в жилище.
2. Закон должен заранее определять устройство, период и вид изымаемых данных.
3. Выгрузка архива в полном объёме не отвечает требованию соразмерности, а отсутствие в законодательстве порядка отбора сведений лишает доступ правового характера, оставляя лишь техническую возможность.
4. Необходимо выровнять порядок доступа к домашнему цифровому архиву с порядком осмотра и обыска жилища.

Проведенный анализ норм уголовно-процессуального законодательства позволил сформулировать следующие изменения и дополнения в УПК:

Дополнить статью 204[1] УПК частью о дистанционном осмотре компьютерной информации, созданной устройствами, установленными в жилище либо обслуживающими жилище, если эта информация хранится вне квартиры (облачный архив, учётная запись голосового помощника, запись внешнего регистратора, связанного с конкретным жилым помещением). Осмотр проводить по постановлению следователя или органа дознания с санкции прокурора либо его заместителя; в случае, не терпящем отлагательства, – с сообщением прокурору в течение двадцати четырёх часов.

ЛИТЕРАТУРА

1. Уголовно-процессуальный кодекс Республики Беларусь [Электронный ресурс]: 16 июля 1999 г. № 295-З : в редакции Закона Республики Беларусь от 17 февраля 2025 г. № 61-З // Эталон. Законодательство Республики Беларусь. – Минск, 2026.
2. Конвенция о защите прав человека и основных свобод : заключена в г. Риме 4 ноября 1950 г. – Текст : электронный // Европейский суд по правам человека : [сайт]. – URL: https://www.echr.coe.int/documents/d/echr/convention_eng (дата обращения: 13.09.2026).
3. Särgava v. Estonia : постановление Европейского суда по правам человека от 16 ноября 2021 г., жалоба № 698/19. – Текст : электронный // HUDOC : база данных Европейского суда по правам человека. – URL: https://hudoc.echr.coe.int (дата обращения: 13.09.2026).
4. Podchasov v. Russia : постановление Европейского суда по правам человека от 13 февраля 2024 г., жалоба № 33696/19. – Текст : электронный // HUDOC : база данных Европейского суда по правам человека. – URL: https://hudoc.echr.coe.int (дата обращения: 13.09.2026).
5. Černý and Others v. the Czech Republic : постановление Европейского суда по правам человека от 18 декабря 2025 г., жалобы № 37514/20 и др. – Текст : электронный // HUDOC : база данных Европейского суда по правам человека. – URL: https://hudoc.echr.coe.int (дата обращения: 13.09.2026)