подпадающих под действие ст. 356 УК. Решение этих вопросов будет способствовать как эффективному противодействию шпионажу, так и соблюдению принципов законности и справедливости уголовного преследования. Перспективным направлением развития законодательства видится также более четкая регламентация ответственности за кибершпионаж с учетом специфики данного способа посягательства на государственную тайну.

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. Закона Респ. Беларусь от 20.10.2025 г. // Национальный правовой Интернет-портал Республики Беларусь. Режим доступа: https://pravo.by/document/?guid=3871&p0=hk9900275 Дата доступа: 05.11.2025.

2. Бабий, Н.А. Уголовная ответственность за преступления против государства / Н.А. Бабий. – Минск: Амалфея, 2019. – 320 с.

3. Уголовный кодекс Республики Беларусь: научно-практический комментарий / под ред. В.М. Хомича. – Минск: ГИУСТ БГУ, 2021. – 784 с.

4. О государственных секретах [Электронный ресурс] : Закон Республики Беларусь от 19 июля 2010 г. № 170-З : в ред. от 29 мая 2025 г. № 80-З : с изм. и доп. от 1 июня 2025 г. // Национальный правовой Интернет-портал Республики Беларусь. Режим доступа: https://pravo.by/document/?guid=3871&p0=H11000170 Дата доступа: 05.11.2025.

ОСОБЕННОСТИ УСТАНОВЛЕНИЯ ПРИЧИННОЙ СВЯЗИ ПРИ ХИЩЕНИИ ПУТЕМ МОДИФИКАЦИИ КОМПЬЮТЕРНОЙ ИНФОРМАЦИИ: АКТУАЛЬНЫЕ ПРОБЛЕМЫ ДОКАЗЫВАНИЯ В УСЛОВИЯХ ПОСТОЯННОГО ИЗМЕНЕНИЯ ЦИФРОВЫХ ТЕХНОЛОГИЙ

Орёл Д.С.,
магистрант ВГУ имени П.М. Машерова, г. Витебск, Республика Беларусь
Научный руководитель – Стаценко В.Г., канд. ист. наук, доцент

Ключевые слова. Причинно-следственная связь, компьютерная информация, модификация, хищение, цифровая реконструкция.

Keywords. Cause and effect, computer information, consciousness, causality, modification, theft, digital reconstruction.

Актуальность темы исследования определяется значимостью глобальных связей в развитии информационных технологий в современных условиях. Благодаря наличию колоссальных соединений в самоорганизующейся информационной системе, которые как нейроны взаимодействуют между собой, установление причинно-следственной связи между деянием и его последствиями в цифровом пространстве является одной из ключевых проблем современной юридической и технической практики. Это связано с особенностями цифровых технологий, а также с высокой степенью анонимности и сложностью технической инфраструктуры. Представляется, что причинно-следственная связь может существовать на уровне кодовой зависимости между элементами физической системы.

Цель исследования состоит в анализе особенностей сбора доказательств установления причинно-следственной связи при совершении хищений путём модификации компьютерной информации.

Материал и методы. Материалом исследования выступает уголовное законодательство Республики Беларусь, а также научные публикации по теме. Методологическую основу составили аналитический, логический, системный, описательный методы научного познания.

Результаты и их обсуждение. За хищение путем использования компьютерной техники предусмотрена уголовная ответственность на основании статьи 212 Уголовного кодекса Республики Беларусь (далее – УК) [1]. Согласно разъяснениям Верховного Суда Республики Беларусь в Постановлении Пленума Верховного Суда Республики Беларусь от 21.12.2001 № 15 «О применении судами уголовного законодательства по делам о хищениях имущества», данное хищение возможно совершить лишь посредством компьютерных манипуляций, заключающихся в обмане потерпевшего или лица, которому имущество вверено или под охраной которого оно находится, с использованием

системы обработки информации. Рассматриваемое хищение может быть совершено как путем изменения информации, обрабатываемой в компьютерной системе, хранящейся на машинных носителях или передаваемой по сетям передачи данных, так и путем введения в компьютерную систему ложной информации [2].

Рассматривая техническую сторону модификации компьютерной информации, нельзя не упомянуть об основных способах данного воздействия: уязвимости в приложениях; компрометация учётных записей администраторов (фишинг, подбор паролей, кража MFA-токена); инсайдерские операции (сотрудник сознательно меняет данные).

Для квалификации действий лица как хищение необходимо достоверно установить причинную связь между модификацией компьютерной информации и наступившим имущественным ущербом. Любые действия по изменению первоначального кода и, соответственно, оставленные цифровые следы носят фрагментарный характер и требуют сложного анализа для установления причинной связи. Действия в цифровой среде могут происходить через промежуточные сервисы и устройства [3, с. 489].

В реальной практике не хватает экспертиз нужного уровня, то есть не все специалисты способны детально восстановить логи, доказать связь изменения информации с конкретной транзакцией. Есть несколько причин, объясняющих сложность в доказывании наличия причинно-следственной связи:

1) после внедрения вредоносной программы преступник часто получает административные права и «чистит» логи - вручную или скриптом, иногда подменяет временные метки и контрольные суммы, что делает хронологию неполной или противоречивой;

2) чем больше прошло времени с момента совершения преступления и началом расследованием, тем выше риск потери данных;

3) в асинхронных репликах порядок применения транзакций может меняться. Это затрудняет точное установление момента изменения.

По данной категории преступлений не в полной мере в законодательстве отражена совокупность доказательств, которая была бы достаточной для однозначного установления причинной связи между модификацией и завладением имущества.

Таким образом, сложность в доказывании наличия причинно-следственной связи возникает в случае, когда между действием правонарушителя и наступившими последствиям имеют место самостоятельные действия информационной системы при несанкционированном доступе к ней либо действия физического лица как реакция на модификацию компьютерной информации. Иными словами, между модификацией данных и фактическим хищением обычно есть цепочка технических событий: серверная обработка, автоматические транзакции, проверка банком. Чтобы доказать, что именно модификация стала непосредственной причиной ущерба, необходимо:

1) восстановить последовательность всех действий в системе (логи, метаданные, временные отметки);

2) доказать, что изменение данных спровоцировало движение средств;

3) исключить альтернативные причины (сбой, ошибка системы, действия третьих лиц).

Заключение. На основании вышеизложенного следует отметить существование определённых сложностей в установлении причинной связи в хищении путём модификации компьютерной информации. Это обуславливается наличием нескольких возможных источников причинения вреда, а также информационная система самостоятельно может отреагировать на посторонний вход. Для эффективного установления причинно-следственной связи в цифровой среде необходима интеграция юридических и технических знаний, развитие экспертных методов и законодательных механизмов.

Только комплексный подход позволит справляться с вызовами, которые ставит перед обществом цифровая эпоха.

1. Уголовный кодекс Республики Беларусь : 9 июля 1999 г. № 275-З : принят Палатой представителей 2 июня 1999 г. : одобр. Советом Респ. 24 июня 1999 г. : в ред. Закона Респ. Беларусь от 17 февраля 2025 г. № 22-З // ЭТАЛОН : информ.-поисковая система (дата обращения: 04.11.2025)

2. О применении судами уголовного законодательства по делам о хищениях имущества [Электронный ресурс]: Постановление Пленума Верховного Суда Республики Беларусь от 21 декабря 2001 г. № 15 : в ред. от 30 сентября 2021 г. №3 // ЭТАЛОН : информ.-поисковая система (дата обращения: 04.11.2025).

3. Орёл, Д.С. Актуальные проблемы установления причинно-следственной связи при совершении деяний в цифровой среде / Орёл Д. С.; науч. рук. Егорова А. Г. // Репозиторий ВГУ имени П. М. Машерова. – URL: https:// conf.vsu.by/wp-content/uploads/2025/10/XIX-машеровские-чтения.-Том-1.pdf (дата обращения: 31.10.2025). – Электрон. версия ст. из: XIX Машеровские чтения : материалы международной научно-практической конф3керенции студентов, аспирантов и молодых ученых, Витебск, 24 октября 2025 г. : в 1 т. – Витебск : ВГУ имени П. М. Машерова, 2025. – Т. 1. – С. 488-489.

ОСОБЕННОСТИ ПРАВОВОГО РЕГУЛИРОВАНИЯ ОБОРОТА ВЗРЫВЧАТЫХ ВЕЩЕСТВ

Орлов Д.А.,
студент 5 курса Псковского государственного университета,
г. Псков, Российская Федерация
Научный руководитель – Гринченко А.Н., ст. преподаватель

Ключевые слова. Взрывчатые вещества, правовой режим, лицензирование, технический регламент, безопасность, административная ответственность, уголовная ответственность.

Keywords. Explosives, legal regime, licensing, technical regulations, safety, administrative liability, criminal liability.

Актуальность изучения правового регулирования оборота взрывчатых веществ обусловлена их двойственной природой. С одной стороны, они критически важны для экономики любого государства, находя применение в горнодобывающей промышленности, строительстве и других отраслях [5]. С другой стороны, их незаконный оборот представляет собой серьёзную угрозу национальной безопасности, общественному порядку и жизни граждан, так как эти вещества зачастую используются при совершении террористических актов и иных тяжких преступлений [8]. Динамичное развитие технологий приводит к появлению новых видов взрывчатых веществ, что требует постоянной адаптации и совершенствования нормативно-правовой базы. Таким образом, комплексный анализ правового регулирования в данной сфере является необходимым условием для выработки эффективных механизмов, обеспечивающих баланс между интересами промышленности и требованиями безопасности.

Целью данного исследования является комплексный анализ современного состояния правового регулирования оборота взрывчатых веществ в Российской Федерации и выявление его специфических особенностей. Для достижения этой цели были поставлены следующие задачи: раскрыть понятие и классификацию взрывчатых веществ как объекта особого правового режима; проанализировать систему нормативно-правовых актов, регулирующих оборот взрывчатых веществ; исследовать административно-правовые и уголовно-правовые средства обеспечения безопасности их оборота; выявить проблемы и перспективы развития законодательства в данной сфере.

Материалы и методы. В качестве материалов и методов исследования были использованы общенаучные и частно-научные методы. Основу работы составил формально-юридический метод, позволивший проанализировать структуру и содержание нормативных правовых актов, таких как Федеральный закон № 116-ФЗ "О промышленной безопасности опасных производственных объектов" [5], Федеральный закон № 99-ФЗ "О лицензировании отдельных видов деятельности" [4], Уголовный кодекс РФ [2] и Кодекс РФ об административных правонарушениях [3]. Сравнительно-правовой метод был применен для сопоставления правовых норм, регулирующих различные аспекты оборота взрывчатых веществ. Системный метод позволил рассмотреть правовое регулирование как целостный механизм.

Результаты исследования и их обсуждение. В российском законодательстве отсутствует единое легальное определение взрывчатых веществ. Содержание выводится из