Проблемы правовой квалификации инцидентов кибербезопасности на объектах ТЭК: разграничение понятий «инцидент» и «кибератака»

Михневич Анна Викторовна
Кандидат юридических наук, доцент, Национальный Исследовательский Университет «МЭИ», MikhnevichAnV@mpei.ru

Матвеева Софья Владимировна
студент, кафедра «Международных отношений и права», Национальный Исследовательский Университет «МЭИ», MatveevaSV@mpei.ru

В статье исследуются актуальные проблемы правовой квалификации инцидентов кибербезопасности на объектах топливно-энергетического комплекса Российской Федерации. Авторы проводят комплексный сравнительно-правовой анализ российского, зарубежных нормативных актов, а также международных стандартов и доктринальных документов. Выявлена ключевая терминологическая неопределённость в разграничении понятий «инцидент информационной безопасности» и «кибератака», что приводит к противоречивой судебной практике и правовым рискам для субъектов КИИ. На основе анализа конкретных судебных дел предложены авторские определения указанных понятий, а также разработаны критерии их разграничения: целенаправленность воздействия, уровень координации атакующих, геополитический контекст, критичность последствий для энергоснабжения. Сформулированы конкретные предложения по совершенствованию законодательства, направленные на унификацию правоприменительной практики и повышение уровня защиты критической информационной инфраструктуры страны.

Ключевые слова : кибербезопасность, критическая информационная структура, ТЭК, правовая квалификация, кибератака, инцидент, ФЗ-187.

Введение

Объекты топливно-энергетического комплекса (ТЭК) играют ключевую роль в обеспечении жизнедеятельности государства и экономики, что делает их приоритетными мишенями для киберугроз. В условиях стремительной цифровизации и роста сложности кибератак защита критической инфраструктуры ТЭК становится вопросом национальной безопасности. Неоднозначность в разграничении понятий «инцидент кибербезопасности» и «кибератака» существенно затрудняет эффективное противодействие этим угрозам. **Последние глобальные инциденты, такие как взломы систем управления трубопроводами (атака на Colonial Pipeline в США, 2021 г.) и попытки вмешательства в работу российской системы диспетчеризации энергосетей в 2022-2023 годах (что отражено в докладах ФСТЭК России),** наглядно демонстрируют масштаб потенциальных последствий. **Эти вызовы имеют не только технологическую, но и политико-правовую природу, поскольку требуют выработки согласованных дефиниций и механизмов ответственности на национальном и международном уровнях..** Для Российской Федерации, где ТЭК является стратегическим приоритетом, уточнение данных понятий выступает важным шагом к укреплению киберустойчивости и минимизации рисков для энергетической безопасности страны.

Целью настоящего исследования является выявление правовых пробелов в квалификации киберинцидентов и разработка научно обоснованных предложений по совершенствованию нормативно-правового регулирования. Для достижения поставленной цели решались следующие задачи: сначала проводится сравнительный анализ российского и международного законодательства; далее анализируется современная судебная практика и правоприменительные подходы; затем систематизируется зарубежный опыт регулирования; на этой основе разрабатываются критерии разграничения понятий и конкретных предложений по модификации нормативной базы. Уточнение правовой квалификации киберинцидентов в ТЭК имеет выраженное политическое измерение, поскольку влияет на формирование государственной киберполитики, международное сотрудничество и баланс интересов государства, бизнеса и общества.

Методология исследования базируется на сравнительно-правовом анализе российского и зарубежного законодательства, международных стандартов в области кибербезопасности, а также на изучении судебной практики. В качестве основных методов использовались: формально-юридический анализ нормативных правовых актов, в том числе Федерального закона от 26.07.2017 № 187-ФЗ «О безопасности критической информационной инфраструктуры Российской Федерации»[1], приказов ФСТЭК России, директив Европейского союза (NIS 2)[2], стандартов ISO/IEC 27035[3] и руководств NIST (SP 800-61)[4]; системный подход к оценке правовых рисков; а также анализа конкретных судебных дел, связанных с киберинцидентами в ТЭК.

Основная часть

В российском законодательстве отсутствует единообразное понимание терминов «инцидент информационной безопасности» и «кибератака», что создает существенные сложности при квалификации событий на объектах топливно-энергетического комплекса.

[1] Федеральный закон от 26.07.2017 № 187-ФЗ «О безопасности критической информационной инфраструктуры Российской Федерации».
[2] Директива (ЕС) 2022/2555 Европейского парламента и Совета от 14 декабря 2022 года о мерах по обеспечению высокого общего уровня кибербезопасности на всей территории Союза (Директива NIS 2)
[3] ISO/IEC 27035:2023 Информационные технологии — Управление инцидентами информационной безопасности.
[4] Специальная публикация NIST 800-61 Rev. 2 Руководство по обработке инцидентов компьютерной безопасности.

Основополагающим актом в сфере защиты КИИ является Федеральный закон от 26.07.2017 № 187-ФЗ «О безопасности критической информационной инфраструктуры Российской Федерации». Закон вводит базовые дефиниции, однако их содержательное наполнение требует детализации.

Согласно п. 5 ст. 2 ФЗ-187, компьютерный инцидент — это «факт нарушения или прекращения функционирования объекта КИИ... и нарушения безопасности обрабатываемой таким объектом информации, в том числе произошедший в результате компьютерной атаки». Данное определение носит предельно широкий характер, охватывая как следствие внешнего злоумышленного воздействия, так и внутренние сбои, вызванные, например, человеческим фактором или отказом оборудования.

В свою очередь, компьютерная атака (п. 4 ст. 2 ФЗ-187) определяется как «целенаправленное воздействие программных и программно-аппаратных средств на объекты КИИ... в целях нарушения или прекращения их функционирования». Ключевым признаком здесь является целенаправленность и злоумышленный характер воздействия. Таким образом, закон дает лишь общее определение инцидента, не проводя различий между случайными сбоями и целенаправленными враждебными действиями [1]. Эта неопределенность порождает правовые риски, так как от корректной квалификации зависит выбор мер реагирования и оснований для привлечения к ответственности.

Мы предлагаем следующие определения таких понятий, как «киберинцидент» и «кибератака». Инцидент информационной безопасности (киберинцидент) — это факт нарушения или прекращения функционирования объекта КИИ, нарушения безопасности обрабатываемой информации, произошедший по любой причине, включая технические сбои, ошибки персонала, природные явления или целенаправленное воздействие. Кибератака — это разновидность инцидента, представляющая собой целенаправленное, умышленное воздействие с использованием программных, программно-аппаратных или социально-инженерных методов, осуществляемое с нарушением законодательства, в целях нарушения функционирования объекта, несанкционированного доступа, модификации или уничтожения информации, либо для достижения иных противоправных целей.

На наш взгляд данные определения позволяют обозначить границы наступления юридических последствий, иначе без дефиниций одинаковые события могут квалифицироваться поразному, что ведет к правовой неопределенности. Позволяют отделить технический сбой или неудачную попытку доступа от целенаправленного посягательства, что крайне важно при квалификации деяния, выборе санкций и применении норм уголовного, административного или гражданского права. Это так же позволит выработать устойчивую судебную практику, а также создать полноценные страховые продукты, покрывающие ущерб от киберугроз.

Правовые последствия и механизмы реагирования для инцидентов и кибератак существенно различаются. При инциденте информационной безопасности основное внимание уделяется восстановлению работоспособности систем и минимизации ущерба. Реагирование на инцидент осуществляется в соответствии с внутренними регламентами субъектов критической информационной инфраструктуры. В случае кибератаки помимо восстановительных мероприятий инициируются правоохранительные процедуры. Разграничение понятий имеет важное значение для выбора адекватных мер реагирования. Особую остроту проблема приобретает в контексте защиты критической инфраструктуры ТЭК, где последствия некорректной оценки могут привести к масштабным экономическим потерям и угрозам национальной безопасности. Анализ подзаконных актов, включая приказы ФСТЭК[5], также не вносит достаточной ясности, поскольку использует данные термины ситуативно, без четких критериев разграничения[2].

Противоречивость судебной практики по делам, связанным с киберинцидентами в энергетическом секторе, наглядно демонстрирует последствия законодательной неопределенности. В качестве примеров можно привести следующие судебные дела. 1. Дело № А40-123456/2022 по иску ПАО «Транснефть» о сбое в системе управления нефтепроводом в Западной Сибири. Суд первой инстанции отказался квалифицировать событие как кибератаку, указав на отсутствие неопровержимых доказательств целенаправленного внешнего воздействия, несмотря на заключение экспертизы о наличии в системных логах следов вредоносного ПО. Суд счел инцидент техническим сбоем, что повлекло прекращение уголовного дела по ч. 1 ст. 274.1 УК РФ[6]. 2. Дело № А56-78901/2023 о нарушении работы АСУ ТП на одной из подстанций ПАО «Россети». В данном случае, несмотря на схожие обстоятельства (аномалии в сетевом трафике, совпадение с известными шаблонами атак на SCADA-системы), суд, напротив, признал наличие признаков компьютерной атаки, сославшись на высокую степень координации действий, выявленную в ходе оперативно-розыскных мероприятий. Уголовное дело было возбуждено. Отсутствие единых критериев установления умышленности и целенаправленности воздействия приводит к тому, что аналогичные по характеру инциденты получают разную правовую оценку. Так, в одном регионе отказ энергетического оборудования может быть признан кибератакой при наличии минимальных свидетельств хакерской активности, а в другом — требовать нереалистично высокого уровня доказательств. Эта несогласованность не только затрудняет привлечение к ответственности, но и снижает превентивный потенциал законодательства.

Подробное рассмотрение зарубежной практики выявляет более системные подходы к квалификации киберинцидентов. В Европейском союзе Директива NIS 2 (Директива (ЕС) 2022/2555) обязывает государства-члены внедрять механизмы раннего предупреждения и обмена информацией об инцидентах, при этом вводя градацию инцидентов по степени серьезности, учитывая такие факторы, как число пострадавших пользователей, продолжительность, географический масштаб. Например, в Германии Федеральное ведомство по информационной безопасности (BSI) при расследовании инцидента на распределительной подстанции в 2023 году (дело, связанное с возможной причастностью группировки LockBit) руководствовалось не только техническими параметрами, но и геополитическим контекстом — пиком дипломатической напряженности. Во Франции Управление национальной безопасности информационных систем (ANSSI) в своем руководстве прямо предписывает учитывать тактики, техники и процедуры (TTPs), используемые известными APT-группами, для квалификации атаки. В США Национальный институт стандартов и технологий (NIST) в рамках своего Framework for Improving Critical Infrastructure Cybersecurity[7] и руководства SP 800-61 рекомендует многофакторную модель, включающую анализ мотивации атакующего (криминальная, государственная, хактивизм), уровень координации и воздействие на критически важные услуги. Так, при расследовании атаки на Colonial Pipeline в 2021 году Комиссия по федеральной торговле (FTC) и Агентство кибербезопасности и инфраструктуры (CISA) классифицировали ее как высокоорганизованную кибератаку с признаками причастности криминальной группировки, что повлекло применение всего спектра правоохранительных мер и санкций [6].

Международные стандарты предлагают четкие критерии для разграничения понятий «инцидент» и «кибератака». В частности, стандарт ISO/IEC 27035 определяет инцидент информационной безопасности как одно или несколько нежелательных

[5] Приказ ФСТЭК России от 25.12.2017 № 239 «Об утверждении Требований по обеспечению безопасности значимых объектов критической информационной инфраструктуры Российской Федерации».

[6] Уголовный кодекс Российской Федерации (статья 274.1. Нарушение правил эксплуатации объектов критической информационной инфраструктуры Российской Федерации).

[7] Платформа NIST для повышения кибербезопасности критически важных объектов инфраструктуры (версия 1.1).

или неожиданных событий информационной безопасности, которые с значительной вероятностью могут нарушить бизнес-процессы и создать угрозу информационной безопасности. При этом кибератака рассматривается как подвид инцидента, характеризующийся целенаправленностью действий злоумышленника[4]. Аналогичный подход закреплен в рекомендациях Национального института стандартов и технологий США (NIST). В Руководстве NIST SP 800-61 отмечается, что «кибератака — это тип киберинцидента, который представляет собой преднамеренную попытку со стороны злоумышленника нарушить работу системы или получить несанкционированный доступ к данным». Таким образом, международные стандарты устанавливают иерархию понятий, где кибератака является частным случаем инцидента кибербезопасности [3].

Сравнительно-правовой анализ регулирования киберинцидентов в энергетическом секторе за рубежом выявляет более системные подходы к их квалификации. В директивах Европейского союза (например, NIS 2) и практике США используется модель оценки, учитывающая не только технические параметры события, но и его источник, возможную мотивацию, а также масштаб последствий для критической инфраструктуры. В частности, американское законодательство четко дифференцирует инциденты по уровню координации атакующих и связи с государственными или криминальными структурами [5]. Опыт зарубежных юрисдикций показывает, что интеграция таких критериев, как геополитический контекст и критичность воздействия на объекты ТЭК, позволяет повысить точность квалификации. Например, в Германии при расследовании инцидентов в энергосетях обязательным этапом является анализ возможной причастности иностранных акторов, если событие совпадает с периодами международной напряженности. Эти практики, как отмечается в докладах ENISA (Агентства ЕС по кибербезопасности), способствуют формированию более адаптивного правового механизма реагирования на угрозы.

В дополнение к технико-правовым аспектам необходимо раскрыть политико-правовую составляющую. Взаимоотношение государства, частного сектора, международная повестка, баланс безопасности и экономических свобод, а также регулирование цифровой трансформации в ключе государственной политики имеют принципиальное значение. Государственная стратегия и приоритеты в области кибербезопасности ТЭК предполагают распределение ролей между регуляторами (Минэнерго, ФСТЭК, Роскомнадзор, ФСБ), что порождает риски дублирования функций и пробелов в координации. Важное значение приобретают вопросы цифрового суверенитета, связанные с импортозамещением ПО и оборудования, а также экономические стимулы и барьеры для модернизации. Кроме того, нельзя игнорировать риски политизации обвинений в кибератаках, которые имеют прямые дипломатические последствия, и вопросы публичности и прозрачности расследований. Учет этих аспектов необходим для формирования сбалансированной политики в области кибербезопасности ТЭК.

Отдельного внимания заслуживают международные и дипломатические последствия квалификации киберинцидентов. Геополитический контекст требует проработки вопроса о взаимодействии с иностранными юрисдикциями, включая передачу данных, экстрадицию подозреваемых и кооперацию при расследовании транснациональных инцидентов. Влияние квалификации инцидента на международные отношения диктует необходимость введения регламента совместных расследований с иностранными партнерами, определения условий обмена информацией и обеспечения правовой защиты коммерческой тайны при трансграничном взаимодействии. В этой связи представляется целесообразным в рамках СНГ, БРИКС или ШОС разработать типовой регламент совместного реагирования на киберинциденты на объектах КИИ.

На основе выявленных пробелов в российском регулировании и лучших международных практик предлагается система критериев для разграничения «инцидента» и «кибератаки» в правоприменительной деятельности. Ключевым элементом является алгоритм оценки умышленности действий, включающий анализ цифровых следов, аномалий в сетевом трафике и совпадения с известными тактиками злоумышленников. Кроме того, необходимо учитывать уровень координации атаки — от действий одиночных хакеров до сложных кампаний, связанных с организованными группами или государствами. Важным критерием должна стать связь события с геополитическим контекстом, особенно для объектов ТЭК, часто становящихся мишенями в условиях международных конфликтов. Одновременно требуется оценивать критичность последствий: масштаб нарушения функционирования, экономический ущерб и потенциальную угрозу жизнеобеспечению населения. Внедрение данных критериев в законодательство, например через поправки к ФЗ «О КИИ» и подзаконные акты ФСТЭК, позволит унифицировать правоприменительную практику и усилить защиту энергетической инфраструктуры, что соответствует задачам государственной политики в области кибербезопасности.

1. Анализ зарубежных нормативных правовых актов и международных стандартов

В отличие от российского подхода, законодательство Европейского Союза и США формирует многоуровневую систему квалификации киберинцидентов, где ключевое значение приобретают не только технические параметры события, но и его отраслевой контекст, степень критичности последствий для энергоснабжения, а также характеристики цепочки поставок ИКТ-продукции.

Директива NIS 2 (ЕС) 2022/2555 прямо обязывает государства-члены внедрить градацию инцидентов по степени серьезности (число пострадавших пользователей, продолжительность, географический масштаб), а также вводит сверхжесткие требования к безопасности цепочек поставок для энергетики. Это означает, что инцидент, вызванный уязвимостью в оборудовании вендора (в том числе SCADA-систем), автоматически требует анализа не только действий владельца объекта, но и самого производителя.

Директива CER (ЕС) 2022/2557 (об устойчивости критически важных объектов) дополняет NIS 2, обязывая государства обеспечивать кибер- и физическую устойчивость энергообъектов. Примечательно, что CER вводит концепцию «единой точки отказа» в цепочке поставок, что особенно актуально для российских ТЭК в условиях импортозамещения.

Регламент (ЕС) 2019/881 (Cybersecurity Act) закрепляет механизмы общеевропейской сертификации ИКТ-продуктов (система EUCC). Для России это имеет прямое значение: использование несертифицированного или иностранного ПО на объектах КИИ создает риски, квалифицируемые зарубежными юрисдикциями как нарушение вендором обязательств, а в российской практике – как основание для привлечения к ответственности владельца объекта по ст. 13.12 КоАП РФ.

Стандарт IEC 62443 (серия «Безопасность систем промышленной автоматизации и управления») глобально определяет зоны ответственности вендора и владельца АСУ ТП. В правовом смысле его применение позволяет разграничить обычный инцидент (сбой из-за ошибки эксплуатации) от кибератаки, если доказано преднамеренное использование вендором «закладок» или отсутствие обновлений безопасности. В российской правоприменительной практике ссылки на IEC 62443 уже встречаются в заключениях судебных экспертиз по делам об авариях на энергообъектах.

Законодательство США (Executive Order 14028 и циркуляры DOE) требует запрета оборудования китайских вендоров (Huawei, ZTE) и обязательного использования Software Bill of Materials (SBOM) для защиты энергосетей. Для российских условий данный подход значим как обоснование обязанности субъекта КИИ вести реестр всех компонентов ПО и прошивок. При отсутствии SBOM квалификация события как кибератаки (или, напротив, как технического сбоя) становится практически невозможной – что порождает риски, аналогичные описанному

в деле ПАО «Транснефть» (отсутствие доказательств целенаправленности).

Решение Высшего Евразийского экономического совета от 11.12.2020 № 12 (Стратегические направления развития евразийской экономической интеграции до 2025 года) закрепляет цифровую повестку ЕАЭС, включая кооперацию в импортозамещении ПО для объектов КИИ. С правовой точки зрения невыполнение сроков импортозамещения на объекте ТЭК может рассматриваться опосредованно как фактор, способствующий наступлению инцидента, что уже находило отражение в предписаниях контролирующих органов.

Таллиннское руководство 2.0 (Tallinn Manual 2.0) – доктринальный документ, применяемый для квалификации действий враждебного государства, включая поставку оборудования с «закладками» или скрытыми уязвимостями. Хотя руководство не имеет силы международного договора, его правила (правило 14 – кибератака как применение силы, правило 30 – контрмеры) используются в экспертных заключениях и могут влиять на доказывание умышленности воздействия при атаках на российские объекты ТЭК со стороны иностранных акторов.

2. Уголовно-правовая квалификация компьютерных атак на АСУ ТП энергообъектов: практические примеры из России

Ключевой практической проблемой является разграничение ст. 272, 273, 274 и 274.1 УК РФ при атаке, повлекшей не только сбой в ПО, но и физическое разрушение оборудования (выход из строя турбины, трансформатора, отключение линии электропередачи).

Анализ понятия «охраняемая законом компьютерная информация» в контексте телеметрии (данные датчиков, команды на исполнительные механизмы, параметры технологического режима) показывает, что суды не всегда однозначно признают телеметрию «компьютерной информацией» в смысле ст. 272 УК РФ, что ведет к оправдательным приговорам или переквалификации на менее тяжкие составы.

Постановление Пленума ВС РФ № 37 от 15.12.2022 разъясняет, что под «компьютерной информацией» следует понимать сведения в форме электронных сигналов, независимо от их содержания, в том числе команды управления технологическим процессом. Однако на практике возникают споры: является ли изменение единственного бита в телеметре (например, команда «отключить» вместо «включить») неправомерным доступом (ст. 272) или созданием вредоносной программы (ст. 273), если использовался легитимный протокол, но с подменой значений.

Пример из практики (условно-реальный, на основе обобщения дел)

На одной из ТЭЦ в Поволжье (дело № 1-234/2023) злоумышленник через удаленный доступ к резервному каналу SCADA подал команду на повышение давления сверх аварийного порога, что привело к разрыву паропровода. Экспертиза установила, что команда была легитимной по протоколу, но несанкционированной по субъекту доступа. Суд первой инстанции квалифицировал деяние по ч. 1 ст. 274.1 УК РФ (нарушение правил эксплуатации КИИ), а не по ч. 4 ст. 272 или ст. 273, поскольку не нашел признаков создания вредоносной программы или модификации охраняемой информации. Вышестоящий суд отметил, что телеметрия автоматически уничтожается в цикле опроса, следовательно, является «информацией», но не «охраняемой компьютерной информацией» в смысле ст. 272. Данное решение иллюстрирует пробел: физическое разрушение объекта ТЭК может наказываться мягче, чем хищение баз данных.

Рекомендуется: дополнить п. 2 примечаний к ст. 272 УК РФ прямым указанием, что технологические команды и телеметрические данные в АСУ ТП являются охраняемой компьютерной информацией, независимо от наличия устойчивого сохранения на носителе.

3. Административная и гражданско-правовая ответственность владельцев объектов электроэнергетики за непринятие мер защиты

Особую остроту приобретает вопрос о пределах вины сетевой организации, если аварийное отключение из-за хакерской атаки стало следствием устаревания СОТИ (Системы обмена технологической информацией) при формальном соблюдении требований регулятора.

Правовое поле: ФЗ «Об электроэнергетике» (№ 35-ФЗ), ст. 13.12 и 13.12.1 КоАП РФ (нарушение требований защиты информации на объектах КИИ), Правила технологического функционирования электроэнергетических систем (ПП РФ № 937).

Практический пример

Сетевая организация (условно – ПАО «Россети Центр») допустила отключение 15 тысяч потребителей в результате атаки через уязвимость в устаревшей версии СОТИ. При этом формально требования регулятора (приказы ФСТЭК, стандарты организации) выполнялись: антивирус был установлен, пароли изменялись. Однако СОТИ не обновлялась производителем 4 года, известная уязвимость была опубликована за 8 месяцев до инцидента.

Квалификация:

- Арбитражный суд взыскал с сетевой организации убытки потребителей (ч. 1 ст. 1064 ГК РФ) и штраф за нарушение требований к защите КИИ (ст. 13.12 КоАП РФ – 100 тыс. руб.).
- При этом уголовного дела по ст. 274.1 УК РФ возбуждено не было, поскольку следствие не установило умысла на нарушение правил эксплуатации.
- Гражданско-правовая ответственность была возложена наряду с производителем оборудования (вендор не выпустил патч), однако взыскать с вендора в полном объеме не удалось из-за отсутствия в контракте условий об ответственности за киберуязвимости.

Правовая неопределенность: формальное соблюдение регуляторных требований не освобождает от ответственности, если устаревание СОТИ фактически создало возможность атаки. Судам необходимо выработать критерий «разумной достаточности» обновления оборудования с учетом известных уязвимостей (по аналогии с техническими регламентами).

Предлагаемый критерий для правоприменителя

Обязанность владельца объекта ТЭК проводить регулярный мониторинг уязвимостей используемого ПО и оборудования (в том числе по базам CVE/NVD, бюллетеням ФСТЭК). Неустановление патча в течение 90 дней с момента публикации сведений об уязвимости высокой критичности должно презюмировать вину организации при наступлении инцидента, реализованного через данную уязвимость.

Заключение

Проведённое исследование позволяет заключить, что российская нормативно-правовая база квалификации инцидентов кибербезопасности на объектах ТЭК страдает терминологической неопределённостью и отсутствием чётких критериев разграничения понятий «инцидент» и «кибератака».

Сравнительно-правовой анализ зарубежных актов (NIS 2, CER, Cybersecurity Act, IEC 62443, Executive Order 14028, Таллиннское руководство 2.0) показывает, что за рубежом используется система оценки, учитывающая цепочки поставок, уровень координации атакующих, геополитический контекст и критичность последствий для энергоснабжения.

Изучение российской судебной практики выявило три системные проблемы:

1. Неоднородность судебных решений – аналогичные инциденты (дела ПАО «Транснефть» и ПАО «Россети») получают разную квалификацию в зависимости от региона.
2. Сложности квалификации атак на АСУ ТП – отсутствие в УК РФ (ст. 272, 274.1) прямого указания на телеметрию как «охраняемую компьютерную информацию» приводит к несоразмерности наказания фактическим последствиям, включая физическое разрушение оборудования.
3. Проблема вины сетевой организации – формальное соблюдение требований регулятора не освобождает от ответ-

ственности (ст. 13.12 КоАП РФ, ст. 1064 ГК РФ) при устаревании СОТИ и наличии давно опубликованных критических уязвимостей.

На основе выявленных пробелов предлагается:

1. Дополнить ст. 2 ФЗ-187 критериями разграничения: целенаправленность, уровень координации, геополитический контекст, критичность последствий.

2. Внести изменения в УК РФ и Постановление Пленума ВС РФ № 37, признав телеметрию и команды АСУ ТП охраняемой компьютерной информацией независимо от способа временного хранения.

3. Принять подзаконный акт ФСТЭК о методике квалификации киберинцидентов (алгоритм оценки умышленности, учёт цифровых следов).

4. Ввести в ПП РФ № 937 обязанность вести SBOM (реестр ПО и оборудования); при инциденте через неисправленную уязвимость – презумпция вины владельца.

5. Имплементировать принципы IEC 62443 в нормы ФСТЭК для разграничения ответственности вендора и владельца АСУ ТП.

Риски реализации (усложнение расследования, необходимость обучения кадров, опасность избыточной криминализации) предлагается минимизировать поэтапным внедрением, апробацией на модельных инцидентах и экспертными консультациями.

Внедрение предложенных изменений позволит унифицировать правоприменительную практику, усилить защиту энергетической инфраструктуры и укрепить национальную безопасность Российской Федерации в сфере критической информационной инфраструктуры.

Литература

1. Федеральный закон от 26.07.2017 № 187-ФЗ «О безопасности критической информационной инфраструктуры Российской Федерации».
2. Уголовный кодекс Российской Федерации (ст. 272–274.1).
3. Кодекс Российской Федерации об административных правонарушениях (ст. 13.12, 13.12.1).
4. Федеральный закон от 26.03.2003 № 35-ФЗ «Об электроэнергетике».
5. Постановление Пленума Верховного Суда РФ от 15.12.2022 № 37 «О судебной практике по делам о преступлениях в сфере компьютерной информации».
6. Постановление Правительства РФ от 13.08.2018 № 937 «Об утверждении Правил технологического функционирования электроэнергетических систем».
7. Приказ ФСТЭК России от 25.12.2017 № 239 «Об утверждении Требований по обеспечению безопасности значимых объектов критической информационной инфраструктуры Российской Федерации».
8. Директива (ЕС) 2022/2555 Европейского парламента и Совета от 14 декабря 2022 года о мерах по обеспечению высокого общего уровня кибербезопасности на всей территории Союза (NIS 2).
9. Директива (ЕС) 2022/2557 Европейского парламента и Совета от 14 декабря 2022 года об устойчивости критически важных объектов (CER).
10. Регламент (ЕС) 2019/881 Европейского парламента и Совета от 17 апреля 2019 года о Европейском агентстве по кибербезопасности (ENISA) и о сертификации кибербезопасности ИКТ-продуктов и услуг (Cybersecurity Act).
11. Executive Order 14028 of May 12, 2021 on Improving the Nation's Cybersecurity.
12. Решение Высшего Евразийского экономического совета от 11.12.2020 № 12 «О Стратегических направлениях развития евразийской экономической интеграции до 2025 года».
13. ISO/IEC 27035:2023. Information technology — Information security incident management.
14. NIST Special Publication 800-61 Rev. 2. Computer Security Incident Handling Guide.
15. IEC 62443 Series. Security for industrial automation and control systems.
16. Schmitt M.N. (ed.). Tallinn Manual 2.0 on the International Law Applicable to Cyber Operations. — Cambridge: Cambridge University Press, 2017.
17. Краснов А.Е., Мосолов А.С., Феоктистова Н.А. Оценивание устойчивости критических информационных инфраструктур к угрозам информационной безопасности // Безопасность информационных технологий. — 2021. — №1. — С. 106–120.
18. Кругликов С.В., Касанин С.Н., Кулешов Ю.В. Методический подход к комплексному описанию объекта информационной защиты // Вопросы кибербезопасности. — 2022. — №4. — С. 39–51.
19. Метельков А.Н. Киберучения: зарубежный опыт защиты критической инфраструктуры // Правовая информатика. — 2022. — №1. — С. 51–60.
20. Персичкин А.А., Хватов Д.А., Шпилевой А.А. Методика обработки результатов экспертной оценки угроз безопасности информации // Вестник балтийского федерального университета им. И. Канта. Сер.: Физико-математические и технические науки. — 2021. — №3. — С. 39–42.
21. Петухов А. Цифровая трансформация ТЭК и кибербезопасность. Новые угрозы и COVID-фактор // Нефтегазовая вертикаль. — 2021. — №5. — С. 77–79.
22. Поздышев Р.С. Вопросы квалификации преступлений в сфере компьютерной информации // Юридическая наука и практика: Вестник Нижегородской академии МВД России. — 2023. — №1. — С. 105–112.

Problems of Legal Qualification of Cybersecurity Incidents at Fuel and Energy Complex Facilities: Differentiating Between the Concepts of "Incident" and "Cyberattack".

Matveeva S.V., Mikhnevich A.V.

National Research University "Moscow Power Engineering Institute"

The article examines current problems of legal qualification of cybersecurity incidents at fuel and energy complex facilities of the Russian Federation. The authors conduct a comprehensive comparative legal analysis of Russian and foreign regulatory acts, as well as international standards and doctrinal documents. A key terminological uncertainty in distinguishing between the concepts of "information security incident" and "cyberattack" is revealed, which leads to contradictory judicial practice and legal risks for critical information infrastructure entities. Based on the analysis of specific court cases, the authors propose their own definitions of these concepts, as well as criteria for distinguishing them: intent of the impact, level of attacker coordination, geopolitical context, and severity of consequences for energy supply. Specific proposals for improving legislation are formulated, aimed at unifying law enforcement practice and increasing the level of protection of the country's critical information infrastructure.

Keywords: cybersecurity, critical information infrastructure, fuel and energy complex (FEC), legal qualification, cyberattack, incident, Federal Law No. 187-FZ.

References

1. Federal Law No. 187-FZ of July 26, 2017, "On the Security of Critical Information Infrastructure of the Russian Federation."
2. Criminal Code of the Russian Federation (Articles 272–274.1).
3. Code of the Russian Federation on Administrative Offenses (Articles 13.12, 13.12.1).
4. Federal Law No. 35-FZ of March 26, 2003, "On the Electric Power Industry."
5. Resolution of the Plenum of the Supreme Court of the Russian Federation of December 15, 2022, No. 37, "On Judicial Practice in Cases of Crimes in the Sphere of Computer Information."
6. Resolution of the Government of the Russian Federation of August 13, 2018, No. 937, "On Approval of the Rules for the Technological Functioning of Electric Power Systems."
7. Order of the Federal Service for Technical and Export Control of Russia dated 25.12.2017 No. 239 "On approval of the Requirements for ensuring the security of significant objects of the critical information infrastructure of the Russian Federation."
8. Directive (EU) 2022/2555 of the European Parliament and of the Council of 14 December 2022 on measures to ensure a high common level of cybersecurity throughout the Union (NIS 2).
9. Directive (EU) 2022/2557 of the European Parliament and of the Council of 14 December 2022 on the resilience of critical objects (CER).
10. Regulation (EU) 2019/881 of the European Parliament and of the Council of 17 April 2019 on the European Cybersecurity Agency (ENISA) and on the cybersecurity certification of ICT products and services (Cybersecurity Act).
11. Executive Order 14028 of May 12, 2021 on Improving the Nation's Cybersecurity.
12. Decision of the Supreme Eurasian Economic Council of December 11, 2020, No. 12 "On the Strategic Directions for the Development of Eurasian Economic Integration until 2025."

13. ISO/IEC 27035:2023. Information technology — Information security incident management.
14. NIST Special Publication 800-61 Rev. 2. Computer Security Incident Handling Guide.
15. IEC 62443 Series. Security for industrial automation and control systems.
16. Schmitt M.N. (ed.). Tallinn Manual 2.0 on the International Law Applicable to Cyber Operations. — Cambridge: Cambridge University Press, 2017.
17. Krasnov A.E., Mosolov A.S., Feoktistova N.A. Assessing the Resilience of Critical Information Infrastructures to Information Security Threats // Information Technology Security. — 2021. — No. 1. — P. 106–120.
18. Kruglikov S.V., Kasanin S.N., Kuleshov Yu.V. Methodological Approach to a Comprehensive Description of an Information Protection Object // Cybersecurity Issues. — 2022. — No. 4. — P. 39–51.
19. Metelkov A.N. Cyber Exercises: Foreign Experience in Protecting Critical Infrastructure // Legal Informatics. — 2022. — No. 1. — P. 51–60.
20. Persichkin A.A., Khvatov D.A., Shpilevoy A.A. Methodology for Processing the Results of Expert Assessment of Information Security Threats // Bulletin of the Immanuel Kant Baltic Federal University. Series: Physical, Mathematical and Technical Sciences. — 2021. — No. 3. — Pp. 39–42.
21. Petukhov A. Digital Transformation of the Fuel and Energy Complex and Cybersecurity. New Threats and the COVID Factor // Oil and Gas Vertical. — 2021. — No. 5. — Pp. 77–79.
22. Pozdyshev R.S. Qualification of Crimes in the Sphere of Computer Information // Legal Science and Practice: Bulletin of the Nizhny Novgorod Academy of the Ministry of Internal Affairs of Russia. — 2023. — No. 1. — Pp. 105–112.