

DOI: 10.17803/1729-5920.2025.227.10.127-145

С. Л. Кисленко

Московский государственный юридический
университет имени О.Е. Кутафина (МГЮА)
г. Москва, Российская Федерация

Киберфизическая модель современного энергетического сектора и актуальные проблемы информационной безопасности

Резюме. В условиях индустрии 4.0 технологический прогресс является главным вектором развития промышленности. Энергетическая отрасль государства стремительно прогрессирует в первую очередь за счет формирования интеллектуальных энергосетей нового поколения, исходящих из передовых двусторонних коммуникаций между элементами электрических сетей, электрическими станциями, аккумулирующими источниками и потребителями (Smart Grid). Однако новая энергетическая концепция передачи и распределения энергии связана с определенными рисками. Среди последних в связи с повышением уровня компьютеризации и интеллектуализации энергетики особое место занимают угрозы кибербезопасности. Энергетические системы России в условиях вооруженного конфликта и санкционной политики всё чаще подвергаются кибератакам. Применительно к функционированию предприятий энергетической сферы одним из ключевых объектов кибератак выступают критические информационные инфраструктуры. С момента СВО данные атаки осуществляются кибернаемниками (и их группировками), которые привлекаются разными недружественными и запрещенными в России структурами в целях дестабилизации энергетической системы нашего государства. Поскольку от функционирования объектов критической информационной инфраструктуры зависит национальная безопасность страны, актуализируются вопросы своевременного пресечения подобных атак.

Ключевые слова: энергетика; национальная безопасность; информационная безопасность; умные сети (Smart Grid); критические информационные инфраструктуры; кибератаки

Для цитирования: Кисленко С. Л. Киберфизическая модель современного энергетического сектора и актуальные проблемы информационной безопасности. *Lex russica*. 2025. Т. 78. № 10. С. 127–145. DOI: 10.17803/1729-5920.2025.227.10.127-145

The Cyberphysical Model of the Modern Energy Sector and Current Problems in Information Security

Sergey L. Kislenko

Kutafin Moscow State Law University (MSAL)
Moscow, Russian Federation

Abstract. In the context of industry 4.0, technological progress is the main vector of industrial development. The state's energy industry is rapidly progressing, primarily due to the formation of new-generation intelligent power grids based on advanced two-way communications between elements of electric networks, electric power plants, storage sources and consumers (Smart Grid). However, the new energy concept of energy transmission and distribution is associated with certain risks. Cybersecurity threats occupy a special place among the latter due to the increasing level of computerization and intellectualization of energy. Russia's energy systems are increasingly being subjected to cyber attacks in the context of armed conflict and sanctions policy. In relation to the functioning of energy sector enterprises, critical information infrastructures are one of the key targets of cyber attacks. Since its launch, these attacks have been carried out by cyber-mercenaries (and their groups), who are attracted by various unfriendly and banned structures in Russia in order to destabilize the energy system of our

© Кисленко С. Л., 2025

state. Since the national security of the country depends on the functioning of critical information infrastructure facilities, the issues of timely suppression of such attacks are becoming relevant.

Keywords: energy; national security; information security; Smart Grid; critical information infrastructures; cyber attacks

Cite as: Kislenko SL. The Cyberphysical Model of the Modern Energy Sector and Current Problems in Information Security. *Lex Russica*. 2025;78(10):127-145. (In Russ.). DOI: 10.17803/1729-5920.2025.227.10.127-145

Введение

Одним из ключевых критериев функционирования современного государства является его способность обеспечивать национальную безопасность. Важной составляющей последней выступает энергетическая безопасность, поскольку обеспечение населения энергией определяет устойчивость развития любого государства, защиту экономических, социальных, экологических и других ресурсов. В Доктрине энергетической безопасности Российской Федерации¹ понятие «энергетическая безопасность» рассматривается через призму состояния защищенности экономики и населения страны от угроз национальной безопасности в сфере энергетики, при котором обеспечивается выполнение предусмотренных отечественным законодательством требований к топливо- и энергоснабжению потребителей, а также выполнение экспортных контрактов и международных обязательств. Такой расширенный подход к пониманию энергетической безопасности во взаимосвязи с остальными элементами национальной безопасности государства вполне обоснован. Объясняется это отчасти тем, что в условиях современных геополитических и экономических вызовов посягательства на состояние стабильного функционирования энергетической системы России наносят ей непоправимый вред. Это может выражаться в экономических потерях (например, падении привлекательности отечественного энергетического сектора для внешних инвесторов, угрозе невыполнения контрактных обязательств и неполучения запланированных доходов), политических (утрате доверия у потенциальных потребителей или транзитных государств), социальных всплесках (из-за падения стабильности обеспечения национальной инфраструктуры энергоресурсами) и пр.

В современных геополитических реалиях — проведение специальной военной операции (СВО) и санкционная политика западных держав в отношении России — именно внешние и трансграничные угрозы ставят отечественную энергетику перед лицом неизбежных инновационных изменений. Они должны быть направлены на обеспечение противодействия угрозам и минимизацию ущерба энергетической сфере, полученного в результате актов незаконного вмешательства. При этом недостаточная готовность организаций энергетического комплекса к функционированию в случае реализации военно-политических вызовов, постоянная модификации технологий террористической и диверсионной деятельности со стороны злоумышленников, стремительное развитие цифровизации и автоматизации производства создают плодородную почву для появления всё новых угроз инфраструктуре и объектам отечественной энергетики.

Анализ «жизнеспособности» объектов энергетики в условиях цифровизации

События последних лет заставляют в целом пересмотреть традиционные подходы к технологиям обеспечения безопасности. На первый план выходит концепция защищенности и жизнеспособности объектов и инфраструктуры (особенно критической) энергетической системы в случае реализации угроз, призванная обеспечить устойчивость таких объектов не только к физическому вмешательству, но и к кибернетическим угрозам.

В этом аспекте серьезным вызовом безопасности в энергетической области являются процессы цифровизации и автоматизации в рамках интеллектуализации ее отраслей. Энергетическая стратегия России на период до 2035 года

¹ Указ Президента РФ от 13.05.2019 № 216 «Об утверждении Доктрины энергетической безопасности Российской Федерации» // СПС «Гарант». URL: <https://www.garant.ru/products/ipo/prime/doc/72140884/#review> (дата обращения: 25.08.2024).

исходит из необходимости внедрения цифровых технологий в электроэнергетику, нефтегазовую, угольную отрасли. В частности, речь идет о поступательном развитии технологии Smart Grid («умная сеть») — интеллектуальных электрических сетей, отражающих связь между разными участниками энергетического рынка (производителями, потребителями, транспортировщиками энергоресурсов). В данной технологии важная роль отводится активно-адаптивным сетям, имеющим принципиально новые свойства. А именно интеллектуальным устройствам, обеспечивающим интеграцию потребителей и поставщиков энергоресурсов в целостную автоматизированную управляемую систему. По сути, речь идет о формировании киберфизических моделей в разных отраслях энергетики, обеспечивающих синтез информационно-коммуникационных и физических (технологических) компонентов в единую управляемую систему. В частности, создание «умных сетей» предусмотрено Стратегией развития электросетевого комплекса Российской Федерации на период до 2030 года². Проект должен пройти последовательные стадии от системы интеллектуального учета Smart Metering до системы «Умный город» (с дистанционным управлением сетями, доступом к информации и ее мониторингом в режиме реального времени, автоматизацией управления интеллектуальными приборами, распределением энергии и самовосстанавливаемостью сетей)³.

С одной стороны, переход электросетей на работу по принципу технологии Smart Grid позволит автоматизировать учет энергоресурсов, тем самым оптимизировать их поток и минимизировать, например, факты хищения. С другой стороны, от работы Smart Grid будет зависеть электроснабжение отдельных террито-

рий, населения, социально значимых объектов, транспортной инфраструктуры и др. При этом усложнение архитектуры электро-энергетических систем за счет функционирования различных взаимозависимых и взаимодействующих между собой компонентов закономерно приводит к увеличению количества потенциальных киберуязвимостей. Следует констатировать, что автоматизация производственных процессов, возможность удаленного управления, несомненно, повышают риски компьютерных атак на объекты информационной инфраструктуры и сети связи, используемые для организации их взаимодействия, способные привести к нарушениям функционирования инфраструктуры и объектов энергетического комплекса.

По данным Kaspersky ICS Cert, в 2021 г. кибератаками было заблокировано 32,4 % компьютеров автоматизированных систем управления (АСУ) в энергетической отрасли по всему миру⁴. Кибератаки в основном реализовывались на уровне аппаратного и программного обеспечения управления компонентами информационно-коммуникационной и технологической систем объектов энергетики в целях нарушения как функции управления, так и работы отдельных объектов энергетики в целом (в частности, для вывода их из строя). Согласно статистике Global Terrorism Database первостепенными целями террористической деятельности в системе топливно-энергетического комплекса (ТЭК) выступают объекты электроэнергетики⁵. Уязвимость электроэнергетических объектов объясняется отчасти тем, что данная отрасль довольно медленно обновляет инфраструктуру и программное обеспечение. По данным отдельных исследований, четверть уязвимостей (25,35 %) в энергетических отраслях связана с отсутствием обновле-

² Внедрение умных сетей происходит в рамках плана мероприятий («дорожной карты») Национальной технологической инициативы по направлению «Энерджинет».

³ Примером может служить концепция цифровой трансформации компании «Россети», в результате которой за 2017–2020 гг. было введено в работу 84 цифровые подстанции, работающие без персонала, 38 цифровых районов электросетей, 22 цифровых центра управления сетями и установлено более 2 млн умных счетчиков (см.: *Заединов А. В.* Перспективы и вызовы цифровой трансформации российской энергетики: от оптимизации до Интернета энергии // Глобальные вызовы и национальные экологические интересы: экономические и социальные аспекты : сборник материалов XVII Междунар. науч.-практ. конференции Российского общества экологической экономики (РОЭЭ/RSEE-2023). Новосибирск : ИЭОПП СО РАН, 2023. С. 238).

⁴ См.: Сектор энергетики стал одной из основных мишеней кибератак // URL: <https://rg.ru/2022/05/17/sector-energetiki-stal-odnoj-iz-osnovnyh-mishenej-kiberatak.html> (дата обращения: 25.08.2024).

⁵ См.: *Лаврухин М.* Терроризм в энергетической промышленности // Энергетическая политика. 2023. № 1. С. 24–37.

ний безопасности. В целом в России уязвима почти половина интернет доступных автоматизированных систем управления⁶. В связи с этим в современной юридической литературе справедливо отмечается, что цифровизация процессов контроля и управления в энергетических отраслях способствует появлению угроз кибернетических атак нового типа, проявляющихся не только в форме несанкционированного доступа к закрытой информации, но и в виде неизвестных ранее возможностей для диверсионных действий на расстоянии, в том числе организуемых с территорий других государств⁷. Яркий пример — сетевой вирус Stuxnet (2010 г.), запущенный с целью поражения автоматизированных систем управления отдельных производств. Вирус использовал уязвимости в ОС Windows, перехватывая и изменяя поток данных электростанций, аэропортов и промышленных предприятий (в частности, для воздействия на блоки управления газовыми центрифугами для получения обогащенного урана на стратегических объектах Ирана⁸). Примером многоступенчатых кибератак может служить семейство вредоносных программ Havex (2014 г.), которые использовались для целенаправленных атак в отношении АСУ компьютерных систем различных отраслей промышленности и получения несанкционированного контроля над ними. Данный вирус заражал официальные дистрибутивы SCADA-систем⁹, которые затем устанавливались на предприятиях, что позволило злоумышленникам получить контроль над АСУ предприятий в нескольких европейских странах¹⁰.

Концепция Smart Grid и интернета вещей в энергетике

Следует констатировать, что устоявшаяся концепция жизнеспособности, которая традиционно применялась к физической защите важнейших объектов инфраструктуры ТЭК, по мере развития цифровых технологий подлежит модификации. В настоящее время она должна включать в себя защиту от кибератак и возможность восстановления работоспособности систем в кратчайшие сроки после киберинцидентов¹¹.

Флагманская роль в обеспечении кибербезопасности объектов энергетики должна отводиться законодательной инициативе, поскольку без модификации нормативных источников практические средства и методы в сфере обеспечения информационной безопасности неэффективны. В данном направлении отечественным законодателем сделан ряд инновационных шагов. В частности, принят Федеральный закон от 26.07.2017 № 187-ФЗ «О безопасности критической информационной инфраструктуры Российской Федерации», следствием чего стало введение в УК РФ статьи 274.1 «Неправомерное воздействие на критическую информационную инфраструктуру Российской Федерации»¹². Установлены требования к обеспечению защиты информации на разных уровнях (диспетчерском, автоматического управления и исполнительных устройств) АСУ критически важных и потенциально опасных объектов производства от неправомерного доступа, уничтожения, модифицирования, блокирования, копирования, предоставления, распространения, а также

⁶ См.: Массель Л. В., Воропай Н. И., Сендеров С. М., Массель А. Г. Кибербезопасность как одна из угроз энергетической безопасности России // Вопросы кибербезопасности. 2016. № 4. С. 2–10.

⁷ См.: Корнеев А. В. Защита инфраструктуры ТЭК от новых средств кибернетического нападения. Опыт борьбы с дистанционным терроризмом // Энергобезопасность и энергосбережение. 2012. № 1. С. 5–10.

⁸ В конце сентября 2010 г. на иранском заводе по обогащению урана Stuxnet вывел из строя около 1 400 из 5 000 центрифуг, в которых шел процесс обогащения радиоактивного сырья.

⁹ SCADA (диспетчерское управление и сбор данных) является одной из ключевых технологий, используемых в Smart Grid. Основными функциями SCADA-системы являются мониторинг, управление и оптимизация работы Smart Grid, что важно для повышения ее эффективности, надежности и устойчивости.

¹⁰ См.: Исследование: уязвимости промышленных систем управления в 2014 году // Хабр. URL: <https://habr.com/ru/companies/pt/articles/258039/> (дата обращения: 11.10.2024).

¹¹ Несмотря на активизацию усилий властей, Россия всё еще далека от лидирующих позиций и занимает 40-е место в Рейтинге сетевой готовности (Network Readiness Index), характеризующем уровень развития информационно-коммуникативных технологий.

¹² Федеральный закон от 26.07.2017 № 194-ФЗ «О внесении изменений в Уголовный кодекс Российской Федерации и статью 151 Уголовно-процессуального кодекса Российской Федерации в связи с принятием Федерального закона “О безопасности критической информационной инфраструктуры Российской Федерации”» // СЗ РФ. 2017. № 31 (ч. I) ст. 4743.

иных неправомерных действий в отношении такой информации, в том числе от деструктивных информационных воздействий (компьютерных атак), следствием которых может стать нарушение функционирования АСУ¹³.

Однако практика правоприменения в анализируемом нами направлении сталкивается с целым рядом проблем как информационного, так и технологического порядка. Среди них — сложность изоляции АСУ предприятий от общей информационной инфраструктуры, что повышает риски внешних воздействий на компоненты АСУ; универсальность используемых в различных АСУ технологий и протоколов, что значительно расширяет возможности и способы несанкционированного проникновения; использование на отечественных предприятиях импортного программного обеспечения, а также отдельных элементов АСУ, содержащихся в открытом доступе в сети Интернет¹⁴. Кроме того, базовые компоненты АСУ (индустриальные протоколы, операционные системы) быстро устаревают и не обновляются¹⁵.

Еще один немаловажный фактор, отмеченный Комитетом ЭСКАТО и связанный с глобальной цифровизацией энергетического сектора, — взаимная зависимость доступа к Интернету и отдельных компонентов энергетических систем (например, «умные» счетчики, «умные» сети, системы диспетчерского управления и сбора данных, а также технологии блокчейн)¹⁶. Как правило, для таких устройств требуется рас-

пределенная автоматизация с помощью высокоскоростной, повсеместной и двусторонней цифровой связи. В современном мире это достигается с помощью технологии интернета вещей (Internet of Things, IoT)¹⁷. Последняя рассматривается как составная часть триады Четвертой промышленной революции — наряду с искусственным интеллектом и большими данными. Данная технология нацелена на объединение цифровой и физической реальности для обеспечения интерактивного сетевого подключения в режиме реального времени к пользователям и устройствам с помощью коммуникационных технологий, а также двустороннего обмена данными между приложениями. В частности, в сфере электроэнергетики технология IoT может быть использована для мониторинга и управления линиями электропередачи и подстанциями, а также отдельным оборудованием; для мониторинга энергосбережения, водоснабжения, температурного режима, освещения, систем мультимедиа в «умных» домах, а также для формирования отчетов¹⁸.

Однако при всей прогрессивности использования IoT в контексте Smart Grid очевидно, что данные технологии повышают риски угроз энергетической безопасности. По сути, Smart Grid в электроэнергетике можно рассматривать как большую киберсистему, включающую физические системы интеллектуальной сети (трансформаторы, выключатели, умные счетчики и т.д.) и интеллектуальные системы кон-

¹³ См.: приказ Федеральной службы по техническому и экспортному контролю от 14.03.2014 № 31 «Об утверждении Требований к обеспечению защиты информации в автоматизированных системах управления производственными и технологическими процессами на критически важных объектах, потенциально опасных объектах, а также объектах, представляющих повышенную опасность для жизни и здоровья людей и для окружающей природной среды» // Российская газета. 06.08.2014. № 175.

¹⁴ См.: *Вериго А. А., Цапко Г. П., Каташев А. С.* Оценка уязвимостей автоматизированных систем управления технологическими процессами // Международный научно-исследовательский журнал. 2016. № 11-4. С. 47–48.

¹⁵ Российские АСУ, пройдя процедуру ввода в эксплуатацию, «опечатаются» и работают без обновлений многие годы. Жесткие регламенты и нормативные акты отдельных предприятий не позволяют вносить в уже сертифицированную систему какие-либо изменения даже в виде обновления операционной системы. В результате уязвимости не устраняются годами.

¹⁶ См.: Материалы третьей сессии Комитета ЭСКАТО по энергетике Экономического и Социального Совета ООН // URL: https://unesco.org/sites/default/d8files/event-documents/CE_2021_1_R.pdf (дата обращения: 06.10.2024).

¹⁷ Технология IoT позволяет обеспечить коммуникацию огромного количества устройств Smart Grid в режиме реального времени посредством единых стандартных протоколов связи (основанных на TCP/IP-совместимости).

¹⁸ См.: *Музыченко Г. Е., Музыченко В. Е., Музыченко В. В.* Применение интернета вещей (IOT) в энергетике // Энергетика: управление, качество и эффективность использования энергоресурсов : сборник трудов X Всерос. науч.-технич. конференции с междунар. участием. Благовещенск, 2022. С. 289.

троля и управления физическими объектами. А поскольку интернет вещей основан на телеметрии и телеуправлении, постольку управление и мониторинг физических объектов происходит дистанционно, как правило при помощи датчиков и сенсоров, подключенных к общему облачному или онлайн-сервису. Уязвимости в данной технологии могут быть использованы преступниками для манипуляций с данными, сгенерированными «умными» объектами. Например, получив несанкционированный доступ к коммуникационным сетям и микропроцессорным устройствам цифровой подстанции, злоумышленник способен привести оборудование к выходу из строя вследствие функционирования подстанции в режиме длительной неустраненной перегрузки.

Кроме того, не все разработчики систем «умный» дом, как и сами потребители, серьезно относятся к их защите. Как показывает практика, злоумышленники, выбрав в Интернете владельца установок Smart Grid, могут легко обойти авторизацию, удаленно установить дефектную прошивку, завладеть доступом к управлению параметрами системы, оказать физические воздействия (вплоть до выведения из строя «умных» устройств — холодильника, печи, кондиционера и пр.)¹⁹.

Как можно заметить, технологии интернета вещей и интернета энергии требуют трансформации устоявшихся средств и методов пресечения угроз информационной безопасности. На первый план выходят технологии защиты, обеспечивающие минимизацию рисков безопасности с учетом следующих основных аспектов: обеспечение информационной безопасности в целом; безопасность приложений; сетевая безопасность; безопасность интернет-приложений; защита ключевых информационных

систем объектов критических инфраструктур. Такой подход всецело отвечает руководящим указаниям в области кибербезопасности — ISO/IEC 27032:2012²⁰. Игнорирование данных ключевых положений информационной безопасности может привести к реальному воплощению киберугроз для современных интеллектуальных сетей и объектов с ними интегрированными. Такие угрозы могут выражаться в невыявленных ошибках в программном обеспечении; злонамеренных программных дефектах в микропроцессорных устройствах АСУ энергетических предприятий; кибератаках через внешние цифровые каналы связи; перехвате каналов телемеханики и телеуправления; ошибках персонала и пр. В результате это может приводить, как отмечается в литературе, к следующим последствиям в энергетических сферах: сбоям в работе алгоритмов функционирования информационных и управляющих систем энергообъектов; управляемым выводам из строя АСУ предприятий; встраиванию зловредного программного кода в системы управления; снятию систем защиты внешних каналов связи; заражению вирусами и др.²¹ В результате исследований отдельными авторами были выделены распространенные угрозы информационной безопасности Smart Grid: 26 % — угрозы на уровне персонала организаций; 30,5 % — на уровне приложений и баз данных; 30,5 % — на уровне сети и 13 % — на уровне мобильных устройств²².

Таким образом, компоненты защиты Smart Grid, по мнению большинства аналитиков, должны охватывать такие аспекты безопасности, как:

а) человеческий фактор — с целью защиты конфиденциальной информации от умышленных или непреднамеренных действий сотрудников или пользователей Smart Grid;

¹⁹ См.: Чайкин А. Чем опасны «умные» электросети // Защита информации. Инсайд. 2015. № 4. С. 40–42.

²⁰ Information technology — Security techniques — Guidelines for cybersecurity. Руководящие указания определяют активы киберпространства и заинтересованные стороны, угрозы, рекомендации и меры по обработке рисков. В качестве специфической меры выделены указания по координации действий и обмену информацией между организациями, формирующими киберпространство, самостоятельные действия которых не обеспечивают эффективную защиту от киберугроз.

²¹ См.: Духвалов А. П. Кибератаки на критически важные объекты — вероятная причина катастроф // Вопросы кибербезопасности. 2014. № 3. С. 50–53 ; Осад А. Б., Панасецкий Д. А., Бузина Е. Я. Влияние кибербезопасности объектов электроэнергетики на надежность функционирования ЭЭС // Методические вопросы исследования надежности систем энергетики // Материалы Междунар. науч. семинара имени Ю.Н. Руденко. Вып. 67. Сыктывкар, 2016. С. 377–385.

²² См.: Пащенко И. Н., Васильев В. И., Гузаиров М. Б. Защита информации в сетях Smart Grid на основе интеллектуальных технологий: проектирование базы правил // Известия ЮФУ. Технические науки. 2015. № 5. С. 28–37.

б) приложения и базы данных — для защиты программных приложений, а также информационно-программных ресурсов и процессов, участвующих в их жизненном цикле;

в) сеть — с целью защиты от угроз, которые могут возникнуть в связи с проектированием и использованием сетей внутри предприятия или между предприятиями, а также между предприятием и пользователями;

г) мобильные устройства — с целью защиты от угроз, связанных с использованием GSM-сетей и мобильных телефонов²³.

Современные угрозы кибербезопасности

Особую опасность среди обозначенных угроз представляют кибератаки. Под компьютерной атакой законодатель понимает целенаправленное воздействие программных и (или) программно-аппаратных средств на объекты критической информационной инфраструктуры, сети электросвязи, используемые для организации взаимодействия таких объектов, в целях нарушения и (или) прекращения их функционирования и (или) создания угрозы безопасности обрабатываемой такими объектами информации²⁴. Целями подобных атак могут быть: создание сбоев в технологических процессах или отключение критически важных энергетических систем; физическое повреждение оборудования; аварии, утечки или даже взрывы на объектах энергетики; нарушение экономической стабильности в регионе; военные диверсии и др. Примером подобных компьютерных атак может служить атака на автоматические выключатели электроподстанций Украины (2015 г.), когда хакеры получили контроль над электросетью (взломав систему SCADA), что привело к массовому отключению подачи электроэнергии.

Интеллектуальная сеть, основанная на технологии IoT, может сталкиваться с целым комплексом компьютерных угроз. Применительно

к функционированию предприятий энергетической сферы одним из ключевых объектов кибератак выступают критические информационные инфраструктуры (КИИ) таких предприятий. Поскольку применительно к данным объектам информационная безопасность тесно переплетается с функциональной, постольку угрозы кибербезопасности могут спровоцировать конкретные физические нарушения в деятельности таких КИИ. Наиболее распространенными целями компьютерных атак являются следующие компоненты КИИ: элементы сбора данных и исполнительные устройства, программные логические контроллеры; автоматизированные системы диспетчерского управления, взаимодействующие с оборудованием, системы, собирающие данные о технологиях, и пр. В связи с этим риски угроз информационной безопасности могут быть связаны с разными уровнями КИИ — буферным (уровень выполнения политик управления), диспетчерским (уровень управления и мониторинга содержательных процессов), терминальным (уровень управления узловыми процессами и оборудованием)²⁵.

При этом риски безопасности многократно возрастают ввиду того, что наибольшее количество кибератак совершаются высокопрофессиональными злоумышленниками. В данной категории с момента СВО следует отдельно выделить кибернаемников (и их группировки), которые привлекаются разными недружественными и запрещенными в России структурами в целях дестабилизации энергетической системы нашего государства. Действия таких лиц в основном направлены на получение несанкционированного доступа к информационным системам организаций и предприятий различных отраслей КИИ для последующего выведения из строя объектов КИИ. Как отметил Президент России В. В. Путин, против нашего государства развязана масштабная война в киберпространстве²⁶. По мнению специалистов Национального координационного центра

²³ См.: Пашенко И. Н., Васильев В. И. Разработка требований к системе защиты информации в интеллектуальной сети Smart Grid на основе стандартов ISO/IEC 27001 и 27005 // Известия ЮФУ. Технические науки. 2013. № 12. С. 117–126.

²⁴ См.: Федеральный закон от 26.07.2017 № 187-ФЗ «О безопасности критической информационной инфраструктуры Российской Федерации» // СЗ РФ. 2017. № 31 (ч. I) ст. 4736.

²⁵ См.: Петухов А. Н., Густин С. Ю. Эталонная модель безопасности критических информационных инфраструктур // Международная конференция по мягким вычислениям и измерениям. СПб. : Санкт-Петербург. гос. электротех. ун-т ЛЭТИ имени В.И. Ульянова (Ленина), 2019. Т. 1. С. 243–246.

²⁶ См.: Путин заявил, что против России развязана война в киберпространстве // ТАСС. URL: <https://tass.ru/politika/14686131> (дата обращения: 09.10.2024).

по компьютерным инцидентам Федеральной службы безопасности России, большинство атак на КИИ российских предприятий, которые проводились из разных стран, были четко скоординированы.

В большинстве своем кибератаки нацелены на IoT-приложения и взаимодействующие с ними АСУ предприятий. Для этого используются: DoS- и DDoS-атаки, сетевые черви, шпионские программы, трояны, вирусы, программы-вымогатели, рекламное ПО, целевой фишинг и пр. Такие атаки могут реализовываться на разных уровнях КИИ предприятий (диспетчерский, терминальный и пр.) в зависимости от их назначения. Например, применительно к современным цифровым подстанциям, наиболее уязвимыми к кибератакам являются компоненты их информационно-коммуникационных подсистем. Атаки на такие подсистемы могут привести к нарушению их управления и развитию аварийных ситуаций. В связи с этим в литературе справедливо отмечается, что прямыми угрозами работоспособности цифровых подстанций являются типовые разновидности кибератак — «отказ в обслуживании» (DoS-, DDoS-атаки), внедрение вирусов и программного обеспечения с «закладками», подмена сигналов GPS и пр.²⁷

И это касается не только промышленных объектов, но и объектов социальной сферы. Практически любое оборудование, подключенное к Интернету или другим сетям передачи данных, подвержено хакерским атакам, так как при его эксплуатации используются программное обеспечение и электронные компоненты, которые потенциально могут содержать уязвимости. В частности, в 2009 г. эксперты компании IOActive пришли к выводам, что контроллеры Smart Grid могут быть использованы для распространения вредоносного кода. Такой код в руках хакеров может быть направлен на

отключение питания через контроллеры Smart Grid посредством функции удаленного отключения, которую поставщики электроэнергии используют для отключения электричества у своих клиентов²⁸. Хакеры могут также получить доступ к связи с диспетчером, к данным с разных датчиков и т.п. Так, в 2024 г. хакерская группировка из Восточной Европы атаковала российские компании через серверы, которые управляли лифтами в подъездах. Злоумышленники взламывали контроллеры, входящие в состав SCADA-систем, и размещали на них серверы, используемые в атаках на другие цели²⁹.

А учитывая, что некоторые устройства в энергетике могут контролироваться и настраиваться удаленно (например, «умные» счетчики или территориально размещенные датчики и приводы в распределительных подстанциях), злоумышленник может попытаться получить несанкционированные права доступа, чтобы использовать их, повреждая физические конкретные объекты (такие как трансформаторы)³⁰.

Компьютерные атаки на интеллектуальные сети зачастую сопряжены с DoS-, DDoS-атаками: злоумышленники перегружают информационную систему, которая перестает отвечать на запросы и пользователи не могут получить к ней доступ. В рамках интернет-электросетей DoS-, DDoS-атаки наиболее опасны в критические часы пик: они ставят под угрозу связь с большинством интеллектуальных счетчиков и при удавшемся отказе системы не позволяют администраторам получить доступ к ней. Примером выступает атака в отношении двух зданий в зимний период в целях их отключения от системы отопления и подачи горячей воды. DoS-атака переполнила поддельным интернет-трафиком систему управления коммуникациями. В результате система бесконтрольно с периодичностью в несколько минут перезагру-

²⁷ См.: Колосок И. Н., Коркина Е. С. Анализ кибербезопасности цифровой подстанции с позиций киберфизической системы // Информационные и математические технологии в науке и управлении. 2019. № 3. С. 121–129.

²⁸ См.: Электросети уязвимы для кибератак // URL: <https://xakep.ru/2009/03/23/47562/> (дата обращения: 09.10.2024).

²⁹ См.: Хакеры атаковали российские компании через взломанные системы для лифтов // РБК. URL: https://www.rbc.ru/technology_and_media/08/07/2024/6687f9af9a7947780a5d1a31?ysclid=m2ybeg8oyv774403520 (дата обращения: 10.10.2024).

³⁰ См.: Довгаль В. А., Довгаль Д. В. Проблемы и задачи безопасности интеллектуальных сетей, основанных на интернете вещей // Вестник Адыгейского государственного университета. Серия : Естественно-математические и технические науки. 2017. № 4. С. 140–147.

жалась, одновременно отказывая администраторам в удаленном доступе³¹.

Особую опасность представляют вредоносные программы, разработанные специально под определенный тип производства или производителя АСУ. Внедрив их в систему, злоумышленник может перехватывать управление технологическими параметрами производства, следствием чего может стать прерывание процессов, порча оборудования или даже опасность для людей и окружающей среды³².

Целью хакеров могут стать также учетные данные клиентов энергетической компании. В том числе и разработчиков систем управления, что не исключает реализацию повторных атак и на другие подобные АСУ аналогичных объектов энергетики.

Наибольшее количество уязвимостей среди компонентов АСУ предприятий энергетики приходится на SCADA-системы (87 % уязвимостей). Фактически на системе SCADA, позволяющей операторам удаленно в режиме реального времени отслеживать сотни различных процессов, держится вся современная промышленность. А поскольку эти системы имеют цифровое управление, постольку они становятся потенциальной мишенью для злоумышленников. Целями последних могут быть:

- нарушение нормальной работы систем SCADA, вызывающее сбой в технологическом процессе или отключение критически важных систем³³;
- причинение физического ущерба (например, изменение параметров управления на

электростанции может привести к перегреву оборудования или механическим отказам, что приведет к физическому повреждению и длительному простоя³⁴);

- криминальные мотивы (скомпрометированная система SCADA может привести к угрозе безопасности персонала, сообществ и окружающей среды — авариям, утечкам или даже взрывам);

- геополитические цели (например, сетевой червь Stuxnet был запущен в 2010 г. для саботажа ядерной программы Ирана путем нанесения физического ущерба его ядерной инфраструктуре)³⁵ и др.

Как правило, основным средством реализации атак на SCADA выступают специально разработанные вредоносные программы, а действия хакеров характеризуются высокой степенью профессиональной подготовки, конспиративностью. При этом начальные фазы таких атак обычно сопряжены с тщательным сбором информации об атакуемом объекте. Впрочем, SCADA-системы зачастую строятся на общедоступных платформах, которые имеют уязвимости. Поэтому, как отмечается в литературе, атаку может провести и начинающий хакер, использующий обычные или специализированные поисковые системы (вроде Shodan³⁶), позволяющие обнаруживать SCADA-системы, доступные через Интернет³⁷.

Кроме того, необходимо учитывать, что к ключевому тренду рынка современных систем HMI³⁸ относятся мобильные устройства, нацеленные на удаленный контроль производствен-

³¹ См.: Панин Д. Н., Бобков Е. О., Балашов Е. А. Анализ кибератак на критическую информационную инфраструктуру с IoT технологиями // Автономия личности. 2020. № 2. С. 58.

³² См.: Петухов А. Как защитить производство от киберугроз // Дайджест «Нефтегаз». 2020. № 17. С. 15.

³³ В 2011 г. хакеры взломали SCADA-системы двух американских ГЭС. В одном из случаев был выведен из строя насос и похищены учетные данные клиентов компании (см.: Хакеры взломали SCADA-систему одной из американских ГЭС // Search inform. URL: <https://searchinform.ru/blog/2011/11/18/hakeri-vzlomali-scada-sistemu-odnoj-iz-amerikanskih-ges/> (дата обращения: 09.10.2024).)

³⁴ В 2011 г. хакеры атаковали компьютерную систему управления одного из локальных американских водоканалов посредством неоднократного включения-выключения управляющей водяными насосами SCADA-системы, что привело к выходу из строя одного насоса (см.: Хакеры атаковали систему управления водоснабжением в США // РИА «Новости». URL: <https://ria.ru/20111118/491983341.html> (дата обращения: 10.10.2024).

³⁵ См.: Небольшой сбой или техногенная катастрофа? Чем так страшны атаки на SCADA // SecurityLab.ru. URL: <https://www.securitylab.ru/analytics/543713.php> (дата обращения: 06.10.2024).

³⁶ Shodan — поисковая система, которая индексирует устройства и сервисы, подключенные к Интернету: веб-камеры, маршрутизаторы, промышленные системы управления, умные устройства и серверы.

³⁷ См.: Яремчук С. Безопасность SCADA // Системный администратор. 2013. № 6. С. 46.

³⁸ HMI (Human Machine Interface) — это интерфейс, который обеспечивает взаимодействие человека с машиной. Если SCADA — это «мозг» системы, то HMI — это ее «лицо», отображающее информацию о работе оборудования в понятном для человека виде и позволяющее управлять им.

ными процессами. Такие технологии позволяют, например, инженеру на своем мобильном устройстве создавать дополнительные экраны, не связанные с экраном панели оператора. С их помощью он может контролировать удаленное оборудование. Одновременно с развитием таких технологий увеличились риски кибернетических угроз. По данным отдельных авторов, второе место среди киберуязвимостей компонентов АСУ предприятий энергетики занимают (наряду с SCADA-системами) системы человеко-машинного интерфейса (49 % от общего количества кибератак)³⁹. При этом более трети уязвимостей HMI (36 %) были связаны с такими инцидентами, как переполнение буфера, что позволяло злоумышленникам вызывать аварийное завершение или «зависание» программ и вело к отказу в обслуживании. При этом отсутствие глобальных стандартов для программного обеспечения HMI еще более усугубляет проблемы безопасности в этом аспекте⁴⁰.

Киберфизические системы и человеческий фактор

Помимо умышленных действий, вред могут причинить действия неумышленные. Главная уязвимость — «кибернеграмотность» персонала предприятий. В частности, сотрудник может пронести на предприятие съемный носитель, который был заражен за пределами сетей предприятия. В результате происходит вторжение вредоносной программы во внутренние системы, когда они подключаются к сетям для сбора данных, обновления ПО контроллеров или сенсоров.

Зачастую у сотрудников отсутствуют достаточные знания для работы с разными типами сетей на предприятии. Особенно халатно работники относятся к корпоративным сетям, поскольку они напрямую не связаны с АСУ

предприятия. Однако на данном уровне их и поджидают злоумышленники. Примером последствий подобной «киберхалатности» может служить кибератака на электросеть в Великобритании в 2017 г., которая была осуществлена с использованием поддельных электронных писем. С помощью фишинговой почты хакеры похитили пароли и ключевую информацию об управлении энергетической сети Великобритании. Целью атаки было выведение из строя сети электропитания путем проникновения в систему SCADA. Этот пример свидетельствует о том, что угрозы информационной безопасности связаны не только с уязвимостями в системах Smart Grid, но и с такими человеческими факторами, как низкая компьютерная грамотность и пренебрежение мерами, обеспечивающими кибербезопасность. Отчасти это обусловлено недостаточным внедрением в энергетический сектор информационного аудита, тестирования на проникновение, сканирования уязвимостей, скрининговых проверок, тренинга персонала и т.д.

Отдельно стоит еще раз упомянуть о Руководящих указаниях по кибербезопасности (ISO/IEC 27032:2012), в пункте которых «Обучение и доведение до сведения персонала» организациям рекомендуется уделять время для повышения компетентности персонала в вопросах кибербезопасности. Содержанием этого обучения должны быть такие вопросы, как фишинг, угрозы из социальных сетей, причины атак и роль сотрудников в борьбе с ними, ряд других аспектов информационной безопасности.

Политика кибербезопасности

В свете последних геополитических событий и последовавших за ними санкций остро встает вопрос о зависимости отечественной энергетики от зарубежных технологий. По данным

³⁹ См.: Грачкова И. А. Информационная безопасность АСУ ТП: возможные вектора атаки и методы защиты // Безопасность информационных технологий. Т. 25. 2018. № 1. С. 92.

⁴⁰ См.: Информационная безопасность в АСУ ТП: вектор атаки человеко-машинный интерфейс // Хабр. URL: <https://habr.com/ru/articles/340164/> (дата обращения: 06.10.2024). Эту проблему хорошо иллюстрирует факт использования в данный момент на территории РФ Межгосударственного стандарта ГОСТ IEC 60447-2015 «Интерфейс “человек-машина”. Основные принципы безопасности, маркировка и идентификация. Принципы включения» (введен в действие приказом Федерального агентства по техническому регулированию и метрологии от 09.10.2015 № 1510-ст). Очевидно, что за последние 10 лет произошли радикальные изменения в уровне и объеме автоматизации технологических процессов, а также в возможностях SCADA-систем. Последнее требует пересмотра действующих стандартов, поскольку они не отражают современный подход к оптимизации HMI.

отдельных авторов, в различных направлениях энергосектора доля отечественных ПО и АСУ колеблется в пределах 1–15 %⁴¹. Зачастую на рынке присутствует нерусифицированное промежуточное ПО иностранных производителей, что вызывает проблемы с метрологической аттестацией систем в целом. Данные обстоятельства также не могут не учитываться при оценке угроз информационной безопасности. Использование на объектах КИИ импортного аппаратного и программного обеспечения прямо сказывается на их кибербезопасности, поскольку импортные решения зачастую по умолчанию обладают функционалом удаленного доступа производителей к компонентам таких решений, что может использоваться для несанкционированного доступа к ним. Кроме того, зарубежные вендоры в условиях санкционной политики ограничили возможность получения обновлений и продления лицензий на используемые решения⁴².

Позитивной тенденцией в направлении реализации стратегии информационной безопасности энергетического сектора видится законодательная инициатива по обеспечению технологической независимости критической информационной инфраструктуры Российской Федерации⁴³. Для решения этой задачи законодательно закреплено понятие российского ПО, создан Единый реестр российских программ для электронных вычислительных машин и баз данных, а также установлен запрет на допуск иностранного ПО для госза-

купок⁴⁴. Энергокомпании обязаны приобретать российское программное обеспечение и электронные компоненты для внедрения интеллектуальных систем управления электрическими сетями. По данным Минэнерго, к 2030 г. доля импортного электротехнического оборудования в закупках компаний не должна превышать 5 %⁴⁵. Кроме того, к предприятиям КИИ со стороны Федеральной службы по техническому и экспортному контролю (ФСТЭК) будет предъявляться дополнительный набор требований по обеспечению информационной безопасности (аутентификация, аудит безопасности, антивирусы и др.).

ФСТЭК планирует обязать предприятия ТЭК хранить информацию о киберинцидентах в течение 3 лет (сведения о дате и времени начала и окончания атаки, типе угрозы, ее интенсивности, перечне сетевых адресов, являющихся источником угроз, и мерах защиты, которые были приняты)⁴⁶. Представляется, что в совокупности с возможностями SCADA-систем хранить историю данных о работе оборудования сведения о киберинцидентах позволят более корректно выявлять слабые места в работе данных систем, проанализировать скрытые причины аварийных ситуаций, оптимизировать производственные процессы с учетом генезиса киберинцидентов. Одной из проблем является создание достаточного количества центров обработки данных — платформ для накопления и сохранения больших данных.

⁴¹ См.: *Баринова В. А., Девятова А. А., Ломов Д. Ю.* Роль цифровизации в глобальном энергетическом переходе и в российской энергетике // Вестник международных организаций: образование, наука, новая экономика. 2021. Т. 16. № 4. С. 126–145.

⁴² См.: Субъектная защита // Коммерсантъ. URL: <https://www.kommersant.ru/doc/6679041> (дата обращения: 10.10.2024).

⁴³ См.: Указ Президента РФ от 30.03.2022 № 166 «О мерах по обеспечению технологической независимости и безопасности критической информационной инфраструктуры Российской Федерации» // СЗ РФ. 2022. № 14. Ст. 2242.

⁴⁴ См.: Федеральный закон от 27.07.2006 № 149-ФЗ «Об информации, информационных технологиях и о защите информации» // СЗ РФ. 2006. № 31 (ч. I). Ст. 3448 ; постановление Правительства РФ от 16.11.2015 № 1236 «Об установлении запрета на допуск программного обеспечения, происходящего из иностранных государств, для целей осуществления закупок для обеспечения государственных и муниципальных нужд» // СЗ РФ. 2015. № 47. Ст. 6600.

⁴⁵ См.: Минэнерго спрогнозировало срок замещения критических технологий в энергетике // Ведомости. URL: <https://www.vedomosti.ru/business/articles/2022/11/09/949431-srok-zamescheniya-kriticheskikh-tehnologii-v-energetike> (дата обращения: 06.10.2024).

⁴⁶ См.: Хранение данных обезопасят требованиями // Коммерсантъ. URL: <https://www.kommersant.ru/doc/6866086> (дата обращения: 10.10.2024).

Выводы и рекомендации

Таким образом, учитывая, что угрозы информационной безопасности объектов энергетики могут быть самыми разными (внешними и внутренними, человеческими и кибернетическими и др.), современные средства и меры по обеспечению безопасности функционирования таких объектов должны носить системный и многоуровневый характер.

1. На административном уровне деятельности энергетических предприятий данный аспект связан с внедрением передовых средств и методик в деятельность разных служб в целях решения комплексных задач по обеспечению безопасности как в отношении внешних угроз (физических, кибернетических), так и внутренних (персонала). На уровне HR-отделов это не только повышение «кибернетической грамотности» персонала предприятий, но и внедрение передовых методик скрининговых⁴⁷ проверок при отборе кандидатов на должности. Такие методики позволяют принимать взвешенные решения о том, предоставлять ли работнику доступ к источникам повышенной опасности, документации, информации ограниченного доступа и пр. На уровне IT-отделов ведущая роль в многоуровневой информационной защите объектов КИИ должна отводиться методам интеллектуального анализа угроз⁴⁸, позволяющим проводить исследования киберугроз: понять их генезис, влияние на организацию или отрасль, определять их актуальность для организации, а также предсказывать киберугрозы и разрабатывать меры проактивного реагирования на них.

2. На уровне функционирования объектов КИИ — постоянный мониторинг информации и событий в сфере безопасности; высокая степень автоматизации диагностики и учета аварийных событий; недопустимость использования беспроводного и удаленного доступа к АСУ пред-

приятия без авторизации и аутентификации; введение двухфакторной аутентификации⁴⁹; исключение неконтролируемого подключения сети АСУ к общей сети предприятия или к Интернету; использование отдельных сетей управления или сегментирование сети (разделение промышленного и корпоративного сегментов и доступа пользователей к различным сегментам); мониторинг сетевого трафика на предмет признаков подозрительной или вредоносной активности; контроль удаленного доступа и защита учетных данных пользователей; создание систем комплексной информационной безопасности и пр. Согласно ст. 3 Федерального закона от 26.07.2017 № 187-ФЗ «О безопасности критической информационной инфраструктуры Российской Федерации»⁵⁰ к средствам, предназначенным для обнаружения, предупреждения и ликвидации последствий компьютерных атак и реагирования на компьютерные инциденты, относятся технические, программные, программно-аппаратные и иные средства для обнаружения (в том числе для поиска признаков компьютерных атак в сетях электросвязи, используемых для организации взаимодействия объектов критической информационной инфраструктуры), предупреждения, ликвидации последствий компьютерных атак и (или) обмена информацией, необходимой субъектам критической информационной инфраструктуры при обнаружении, предупреждении и (или) ликвидации последствий компьютерных атак. Это положение предопределяет необходимость постоянного мониторинга кибербезопасности энергетических предприятий, включающего проведение аудита безопасности, выявление критических киберуязвимостей информационно-технологических систем, выработку и реализацию мероприятий по их устранению⁵¹, в частности регулярное тестирование планов реагирования на киберинциденты.

⁴⁷ Скрининг (от английского screening — просеивание, отсеивание) — это процесс проверки кандидата на должность с целью выявления факторов риска, препятствующих качественному выполнению им обязанностей и содержащих угрозы работодателю и коллективу сотрудников в целом.

⁴⁸ Например, Threat intelligence platform — платформа для организации проактивного реагирования на киберугрозы, которая позволяет собирать информацию из различных источников, накапливать ее, обогащать и обрабатывать, систематизировать, профилировать. В частности, она позволяет сортировать инциденты, представлять их в графическом интерфейсе для удобства аналитики и др.

⁴⁹ Как свидетельствует практика, в большинстве киберинцидентов доступ к инфраструктуре систем управления был получен злоумышленниками путем обычного перебора паролей.

⁵⁰ СЗ РФ. 2017. № 31 (ч. I). Ст. 4736.

⁵¹ См.: Массель А. Г., Гуськова Д. А. Методы и подходы к обеспечению кибербезопасности объектов цифровой энергетики // Энергетическая политика. 2018. № 5. С. 62–72.

На уровне проектирования сетей объектов КИИ, удовлетворяющих ICS-стандартам⁵², — зональное разделение ICS-инфраструктуры. В частности, в корпоративных зонах обычно находится корпоративная сеть со стандартными службами (электронная почта, печать, веб и пр.). Данная сеть обеспечивает функционирование серверов, имеющих отношение к бизнесу, рабочим станциям сотрудников. В демилитаризованных зонах (DMZ) обычно находятся вторичные сервера с архивными данными и некоторые веб- и терминальные приложения. Функция такой зоны — защита внутренней сети организации от потенциальных внешних атак. Внешний злоумышленник имеет прямой доступ только к оборудованию в DMZ, при этом внутренние сети остаются защищенными. Зона же управления процессами должна быть полностью изолирована от корпоративной зоны, а со стороны человеко-машинных интерфейсов и SCADA-серверов в зону управления процессами должен быть ограниченный доступ⁵³.

Не менее важное место в данном аспекте должно отводиться методам не только пассивной защиты (брандмауэры, антивирусное программное обеспечение, контроль доступа, установка обновлений и средств реагирования и пр.), но и активной защиты, позволяющей отслеживать злоумышленников и вредоносное программное обеспечение. К одной из разновидностей активных средств защиты в литературе относят введение полумарковских моделей⁵⁴ для анализа распространения последствий кибератак на SCADA-системы и

восстановления после атак. Надежность SCADA-систем будет рассматриваться через призму не только двух ключевых состояний (безотказная работа и отказ), но и дополнительных: нормальное состояние — состояние уязвимости — состояние взлома — состояние активной/пассивной защиты — состояние необнаружения атаки — состояние отказа. В результате реакцию системы на кибервторжения можно будет описать с учетом многофакторных переходных состояний и их взаимосвязей, что позволит более точно определить причины любого нарушения и предпринять адекватные корректирующие действия⁵⁵.

3. На уровне разработки и использования ПО для АСУ предприятий — разработка отечественного ПО с высокой степенью надежности; разработка протоколов безопасности и пр. Представляется, что в условиях современных геополитических реалий приоритет в направлении программного обеспечения объектов КИИ должен отводиться принципу не только надежности, но и автономности⁵⁶.

На административном уровне вышеуказанное положение должно обеспечиваться, с одной стороны, минимизацией административных трудностей для своевременного обновления ПО, а с другой — строгим контролем над использованием на объектах КИИ допустимого ПО. В частности, список разрешенного к использованию ПО должен утверждаться субъектом электроэнергетики, а использование программного обеспечения, не внесенного в список, не должно допускаться⁵⁷.

⁵² Система промышленного контроля (Industrial Control System, ICS) — термин, описывающий интеграцию аппаратного и программного обеспечения с сетевым подключением с целью поддержания работоспособности критически важной инфраструктуры.

⁵³ См.: Введение в безопасность систем ICS/SCADA // SecurityLab.ru. URL: <https://www.securitylab.ru/analytics/487977.php> (дата обращения: 06.10.2024).

⁵⁴ Полумарковская модель — это модель дискретно-непрерывного случайного процесса, в которой изменение времени пребывания системы в каком-либо состоянии является случайным с некоторым законом распределения, а переходы из одного состояния в другие осуществляются мгновенно с определенными вероятностями. Достоинством полумарковских моделей является их аналитический характер, а значит, возможность прогнозирования их поведения на различных временных интервалах и коррекции их параметров с учетом получаемой информации.

⁵⁵ См.: Гурина Л. А. Повышение киберустойчивости SCADA и WAMS при кибератаках на информационно-коммуникационную подсистему ЭЭС // Вопросы кибербезопасности. 2022. № 2. С. 18–26.

⁵⁶ Согласно Указу Президента РФ от 30.03.2022 № 166 с 1 января 2025 г. органам государственной власти, заказчикам запрещается использовать иностранное программное обеспечение на принадлежащих им значимых объектах критической информационной инфраструктур.

⁵⁷ См.: приказ Министерства энергетики РФ от 06.11.2018 № 1015 «Об утверждении требований в отношении базовых (обязательных) функций и информационной безопасности объектов электроэнергетики при создании и последующей эксплуатации на территории Российской Федерации систем удаленного

Технологии SCADA и коммуникационные протоколы должны изначально проектироваться с учетом требований аутентификации, шифрования, утилит против вредоносных программ и других защитных механизмов с учетом современных реалий. В частности, на уровне IoT-приложений, используемых в критических инфраструктурах, — шифрование каналов связи между IoT-устройствами и системой управления; строгая аутентификация устройств (на основе паролей, цифровых сертификатов и пр.) в целях их идентификации и согласование задач, которые такие устройства должны выполнять в сети (в целях предотвращения выполнения несанкционированных команд); регулярное обновление прошивки устройств и др.⁵⁸

Представляется, что в данном направлении приоритет должен отдаваться концепции Security by Design, когда вопросы предотвращения уязвимостей решаются еще на этапе проектирования IoT-устройств путем тщательного анализа потенциальных угроз и разработки превентивных контрмер.

4. На уровне человек — машина требуется повышение эффективности взаимодействия операторов с SCADA-системами. Предпочтителен отказ от пассивного подхода в области разработки HMI, когда интерфейсы разрабатываются по уже используемым образцам⁵⁹. Представляется, что современные интерфейсы SCADA-систем должны не только обеспечивать возможность быстро и четко управлять системой, независимо от ее текущего состояния, условий окружающей среды и других факторов, но и отвечать современным принципам кибербезопасности.

Кроме того, если речь идет об использовании мобильных устройств в качестве HMI, энергетические компании должны заботиться о реализации политики безопасности мобильных устройств, задействованных в сети управ-

ления технологическими процессами: определять действия, которые эти устройства могут выполнять, и время, в течение которого эти действия разрешены; указывать, какие изменения могут быть внесены в устройство, кому разрешено вносить эти изменения и как они могут быть внесены; указывать места и коммуникационные сети, которые эти устройства могут использовать для доступа; определять, как каждое устройство может быть подключено к сети управления технологическим процессом; указывать тип данных, которые могут передаваться, и др.⁶⁰

5. На кадровом уровне — повышение цифровой грамотности пользователей киберфизических систем. В настоящее время справедливо отмечается, что существенным препятствием на пути цифровизации энергетического сектора являются неудовлетворительные навыки персонала по работе с цифровыми технологиями. Как свидетельствуют отдельные исследования, около 71 % энергокомпаний нуждаются в работниках с опытом работы с доменами и цифровыми технологиями, а 18 % не имеют в штате ни одного сотрудника с таким набором навыков⁶¹. По итогам форсайт-исследования, проведенного Российским национальным комитетом Международного совета по большим электрическим системам высокого напряжения в 2018 г. в области наиболее востребованных профессий будущего в электроэнергетике, лидерами стали: специалист по цифровым системам управления энергетических объектов (21,8 %), специалист по обеспечению кибербезопасности предприятий энергетики (21,5 %), системный инженер интеллектуальных энергосетей (16,8 %) и специалист по диагностике и управлению активами энергетических компаний (15,2 %) ⁶².

6. На законодательном уровне должны получить нормативное отражение в первую очередь основные категории, относящиеся к

мониторинга и диагностики энергетического оборудования» // СПС «Гарант». URL: <https://base.garant.ru/72176552/> (дата обращения: 11.10.2024).

⁵⁸ См.: Панин Д. Н., Бобков Е. О., Балашов Е. А. Указ. соч. С. 61.

⁵⁹ Отчасти это объясняется тем, что разработчики решений SCADA (в отличие от операторов и диспетчеров) имеют меньше опыта в отношении построения пользовательского интерфейса.

⁶⁰ См.: ГОСТ Р ИСО/МЭК 27019-2021 «Информационные технологии. Методы и средства обеспечения безопасности. Меры обеспечения информационной безопасности в энергетике (неатомной)» // Росстандарт. URL: <https://protect.gost.ru/default.aspx/document1.aspx?control=31&baseC=6&page=4&month=6&year=2021&search=&id=240763> (дата обращения: 11.10.2024).

⁶¹ См.: Аполлонский С. М. Энергосберегающие технологии в энергетике в России. М. : Русайнс, 2022. С. 309.

⁶² Кадровый вопрос: энергетике не хватает универсальных специалистов / РНК СИГРЭ // URL: <http://www.cigre.ru/news/5/9968/> (дата обращения: 10.10.2024).

технологии Smart Grid, а также вопросы, связанные с разработкой технического регламента для установления на государственном уровне минимально необходимых требований и принципов построения «интеллектуальных сетей»⁶³; со стандартизацией протоколов; с введением обязательств по системам телеметрии и автоматики, а также обязательств производителей по обеспечению безопасности продукции (ПО, IoT-устройств и пр.) и предоставлению информации о рисках (потенциальных уязвимостях) и пр.

7. На уровне деятельности правоохранительных органов должны совершенствоваться технические и методические разработки в области расследования актов кибернетического вмешательства в деятельность объектов КИИ энергетического сектора⁶⁴. Однако данный аспект осложнен рядом факторов. Во-первых, относительной «молодостью» статьи 274.1 УК РФ, обуславливающей, как отмечается в литературе, ограниченность правоприменительной практики по расследованию неправомерного воздействия на критическую информационную структуру Российской Федерации (ст. 274.1 УК РФ) и, как следствие, отсутствие апробированных методических рекомендаций по расследованию и выявлению данных преступлений. Отчасти это объясняется тем, что преступления данной категории имеют большую латентность по сравнению с другими преступными посягательствами, предусмотренными главой 28 УК РФ⁶⁵. Так, в 2022 г. по делам о 519 зарегистрированных таких преступлениях было осуждено 57 человек⁶⁶. При этом речь идет не о профессиональных киберпреступниках, которые нанесли необратимый вред значимым объектам КИИ (ТЭК, транспортной инфраструктуры,

в области атомной энергии, металлургической, химической и другой промышленности), а о рядовых работниках предприятий, которым вменяется осуществление с использованием служебных полномочий неправомерного доступа к компьютерным системам, отнесенным к объектам КИИ. В результате, как отмечается в литературе, на скамье подсудимых по данной статье оказывались работники медицинских учреждений, обвиняемые в оформлении ложных сертификатов о прохождении вакцинации от COVID, которые воспользовались доступом к Единой государственной информационной системе в сфере здравоохранения (ЕГИСЗ); сотрудники салонов связи, оформившие SIM-карты на чужие или вымышленные паспортные данные для выполнения плана продаж (поскольку оператор является субъектом КИИ, а автоматизированная система расчетов значимым объектом КИИ) и пр.⁶⁷

Во-вторых, у сотрудников правоохранительных органов нередко возникают проблемы, связанные с их недостаточной компьютерной грамотностью, отсутствием знаний нормативно-правовой базы, регламентирующей деятельность объектов энергетики, нехваткой материально-технического обеспечения и неумением им пользоваться и др.

Поэтому одной из ключевых задач современного функционирования правоохранительных органов является их кадровое обеспечение. Представляется, что классического юридического образования в реалиях цифрового социума недостаточно. Мы поддерживаем предложение Л. В. Бертовского о введении в образовательные программы дисциплин уголовно-правового профиля, отражающих технический и информационный аспекты данной

⁶³ В том числе в соответствии с требованиями Федерального закона от 27.12.2002 № 184-ФЗ «О техническом регулировании» (СЗ РФ. 2002. № 52 (ч. I) ст. 5140).

⁶⁴ Расследование неправомерного воздействия на критическую информационную структуру Российской Федерации находится в подследственности Федеральной службы безопасности Российской Федерации.

⁶⁵ См.: Голубев Ф. А. Криминалистическая характеристика расследования неправомерного воздействия на критическую информационную структуру Российской Федерации // Право и политика. 2020. № 10. С. 50–59.

⁶⁶ Отчасти проблема заключалась и в том, что с момента введения ст. 274.1 УК РФ на практике складывались ситуации, когда на период совершения общественно опасного деяния — вмешательства в функционирование программных или программно-аппаратных средств — данные объекты не были категоризованы и, соответственно, не были включены ФСТЭК России в реестр значимых объектов КИИ (см.: Малыгин И. И. Уголовно-правовое противодействие неправомерному воздействию на критическую информационную инфраструктуру : дис. ... канд. юрид. наук. М., 2023. С. 81–82).

⁶⁷ См.: Домкин П. Критическая оценка правоприменительной практики по статье 274.1 УК РФ // Information Security. Информационная безопасность. 2022. № 4. С. 4–5.

проблематики (использование в энергетических секторах больших данных, нейротехнологий и искусственного интеллекта, возможностей робототехники и сенсорики, технологий беспроводной связи, виртуальной и дополненной реальности и др.)⁶⁸.

В рамках повышения квалификации работников правоохранительных органов по вопросам расследования компьютерных преступлений в сфере энергетики целесообразно задействовать не только научно-педагогический состав юридических и технических вузов, но и представителей энергетических компаний, а также IT-специалистов и судебных экспертов. Это позволит ознакомить следователей с современными методами и приемами работы специалистов разных направлений; с существующими программными и аппаратными комплексами; средствами, предназначенными для обнаружения, предупреждения и ликвидации киберинцидентов; со специализированными комплексами, предназначенными для крими-

налистического документирования цифровых сведений и их дальнейшего исследования (по типу «Мобильный криминалист»); с описанием источников угроз, типовых уязвимостей, объектов воздействия, моделей типичных нарушителей информационной безопасности, а также их деструктивных действий в отношении объектов КИИ; с разновидностями и возможностями компьютерно-технической экспертизы; с технологией функционирования объектов энергетического комплекса; с принципами работы систем безопасности объектов критической информационной инфраструктуры; с возможностями и направлениями взаимодействия с субъектами критической информационной инфраструктуры и пр.

В любом случае лишь комплексный подход к решению анализируемых проблем позволит судить об эффективности применения средств и методов выявления и пресечения угроз информационной безопасности объектов энергетического сектора.

СПИСОК ЛИТЕРАТУРЫ

- Аполлонский С. М. Энергосберегающие технологии в энергетике в России. М. : Русайнс, 2022. 441 с.
- Баранова В. А., Девятова А. А., Ломов Д. Ю. Роль цифровизации в глобальном энергетическом переходе и в российской энергетике // Вестник международных организаций: образование, наука, новая экономика. 2021. Т. 16. № 4. С. 126–145.
- Бертовский Л. В. О некоторых проблемах расследования преступлений, совершаемых в сфере энергетики // Криминалистические чтения на Слобожанщине : сборник материалов Междунар. науч.-практ. конференции, Белгород, 8 октября 2021 г. / под ред. Н. А. Жуковой. Белгород : БелГУ НИУ «БелГУ», 2021. С. 3–7.
- Вериго А. А., Цапко Г. П., Каташев А. С. Оценка уязвимостей автоматизированных систем управления технологическими процессами // Международный научно-исследовательский журнал. 2016. № 11-4. С. 47–48.
- Духвалов А. П. Кибератаки на критически важные объекты — вероятная причина катастроф // Вопросы кибербезопасности. 2014. № 3. С. 50–53.
- Довгаль В. А., Довгаль Д. В. Проблемы и задачи безопасности интеллектуальных сетей, основанных на интернете вещей // Вестник Адыгейского государственного университета. Серия «Естественно-математические и технические науки». 2017. № 4. С. 140–147.
- Домкин П. Критическая оценка правоприменительной практики по статье 274.1 УК РФ // Information Security. Информационная безопасность. 2022. № 4. С. 4–5.
- Голубев Ф. А. Криминалистическая характеристика расследования неправомерного воздействия на критическую информационную структуру Российской Федерации // Право и политика. 2020. № 10. С. 50–59.
- Грачкова И. А. Информационная безопасность АСУ ТП: возможные вектора атаки и методы защиты // Безопасность информационных технологий. Т. 25. 2018. № 1. С. 90–98.

⁶⁸ Бертовский Л. В. О некоторых проблемах расследования преступлений, совершаемых в сфере энергетики // Криминалистические чтения на Слобожанщине : сборник материалов Междунар. науч.-практ. конференции, Белгород, 8 октября 2021 г. / под ред. Н. А. Жуковой. Белгород : БелГУ НИУ «БелГУ», 2021. С. 6.

Гурина Л. А. Повышение киберустойчивости SCADA и WAMS при кибератаках на информационно-коммуникационную подсистему ЭЭС // Вопросы кибербезопасности. 2022. № 2. С. 18–26.

Заединов А. В. Перспективы и вызовы цифровой трансформации российской энергетики: от оптимизации до интернета энергии // Глобальные вызовы и национальные экологические интересы: экономические и социальные аспекты : сборник материалов XVII Междунар. науч.-практ. конференции Российского общества экологической экономики (РОЭЭ/RSEE-2023). Новосибирск : ИЭОПП СО РАН, 2023. С. 235–240.

Колосок И. Н., Коркина Е. С. Анализ кибербезопасности цифровой подстанции с позиций киберфизической системы // Информационные и математические технологии в науке и управлении. 2019. № 3. С. 121–129.

Корнеев А. В. Защита инфраструктуры ТЭК от новых средств кибернетического нападения. Опыт борьбы с дистанционным терроризмом // Энергобезопасность и энергосбережение. 2012. № 1. С. 5–10.

Лаврухин М. Терроризм в энергетической промышленности // Энергетическая политика. 2023. № 1. С. 24–37.

Малыгин И. И. Уголовно-правовое противодействие неправомерному воздействию на критическую информационную инфраструктуру : дис. ... канд. юрид. наук. М., 2023. 192 с.

Массель Л. В., Воропай Н. И., Сендеров С. М., Массель А. Г. Кибербезопасность как одна из угроз энергетической безопасности России // Вопросы кибербезопасности. 2016. № 4. С. 2–10.

Массель А. Г., Гуськова Д. А. Методы и подходы к обеспечению кибербезопасности объектов цифровой энергетики // Энергетическая политика. 2018. № 5. С. 62–72.

Музыченко Г. Е., Музыченко В. Е., Музыченко В. В. Применение интернета вещей (IoT) в энергетике // Энергетика: управление, качество и эффективность использования энергоресурсов : сборник трудов X Всерос. науч.-технич. конференции с междунар. участием. Благовещенск, 2022. С. 286–290.

Панин Д. Н., Бобков Е. О., Балашов Е. А. Анализ кибератак на критическую информационную инфраструктуру с IoT-технологиями // Автономия личности. 2020. № 2. С. 55–64.

Пащенко И. Н., Васильев В. И. Разработка требований к системе защиты информации в интеллектуальной сети Smart Grid на основе стандартов ISO/IEC 27001 И 27005 // Известия ЮФУ. Технические науки. 2013. № 12. С. 117–126.

Пащенко И. Н., Васильев В. И., Гузаиров М. Б. Защита информации в сетях Smart Grid на основе интеллектуальных технологий: проектирование базы правил // Известия ЮФУ. Технические науки. 2015. № 5. С. 28–37.

Петухов А. Н., Густин С. Ю. Эталонная модель безопасности критических информационных инфраструктур // Международная конференция по мягким вычислениям и измерениям. СПб. : Санкт-Петербургский гос. электротех. ун-т ЛЭТИ имени В.И. Ульянова (Ленина), 2019. Т. 1. С. 243–246.

Петухов А. Как защитить производство от киберугроз // Дайджест «Нефтегаз». 2020. № 17. С. 14–17.

Осак А. Б., Панасецкий Д. А., Бузина Е. Я. Влияние кибербезопасности объектов электроэнергетики на надежность функционирования ЭЭС // Методические вопросы исследования надежности систем энергетики : материалы Междунар. науч. семинара имени Ю.Н. Руденко. Вып. 67. Сыктывкар, 2016. С. 377–385.

Чайкин А. Чем опасны «умные» электросети // Защита информации. Инсайд. 2015. № 4. С. 40–42.

Яремчук С. Безопасность SCADA // Системный администратор. 2013. № 6. С. 44–47.

REFERENCES

Apollonskiy SM. Energy-saving technologies in the energy sector in Russia. Moscow: Rusayns Publ.; 2022. (In Russ.).

Barinova VA, Devyatova AA, Lomov DYU. The role of digitalization in the global energy transition and in the Russian energy sector. *Vestnik mezhdunarodnykh organizatsiy: obrazovanie, nauka, novaya ekonomika*. 2021;16(4):126-145. (In Russ.).

Bertovskiy LV. On some problems of investigating crimes committed in the energy sector. In: Zhukova NA, editor. *Criminalistic readings in Slobozhanshchina: Proceedings of the International Scientific and Practical Conference, Belgorod, October 8, 2021*. Belgorod: National Research University «BelSU»; 2021. P. 3-7. (In Russ.).

Chaykina A. What are the dangers of «smart» power grids. *Zashchita informatsii. Insayd*. 2015;4:40-42. (In Russ.).

- Domkin P. Critical assessment of law enforcement practice under Article 274.1 of the Criminal Code of the Russian Federation. *Informatsionnaya bezopasnost [Information security]*. 2022;4:4-5. (In Russ.).
- Dovgal VA, Dovgal DV. Security issues and challenges of intelligent networks based on the Internet of Things. *Vestnik dygeyskogo gosudarstvennogo universiteta. Seriya «Estestvenno-matematicheskie i tekhnicheskie nauki» [The Bulletin of the Adyghe State University Natural-Mathematical and Technical Sciences Series]*. 2017;4:140-147. (In Russ.).
- Dukhvalov AP. Cyber attacks on critically important objects are a probable cause of disasters. *Voprosy kiberbezopasnosti*. 2014;3:50-53. (In Russ.).
- Golubev FA. Criminalistic characteristics of the investigation of unlawful influence on the critical information structure of the Russian Federation. *Pravo i politika [Law and politics]*. 2020;10:50-59. (In Russ.).
- Grachkova IA. Information security of automated process control systems: Possible attack vectors and protection methods. *Bezopasnost informatsionnykh tekhnologiy*. 2018;25(1):90-98. (In Russ.).
- Gurina LA. Increasing the cyber resilience of SCADA and WAMS during cyber attacks on the information and communication subsystem of the EES. *Voprosy kiberbezopasnosti*. 2022;2:18-26. (In Russ.).
- Kolosok IN, Korkina ES. Analysis of cybersecurity of a digital substation from the perspective of a cyberphysical system. *Informatsionnye i matematicheskie tekhnologii v nauke i upravlenii*. 2019;3:121-129. (In Russ.).
- Korneev AV. Protection of the fuel and energy sector infrastructure from new means of cyber attack. The experience of combating remote terrorism. *Energobezopasnost i energoberezenie*. 2012;1:5-10. (In Russ.).
- Lavrukhin M. Terrorism in the energy industry. *Energeticheskaya politika*. 2023;1:24-37. (In Russ.).
- Malygin II. Criminal law counteraction to unlawful impact on critical information infrastructure. Cand. Diss. (Law). Moscow; 2023. (In Russ.).
- Massel LV, Voropai NI, Senderov SM, Mussel AG. Cybersecurity as one of the threats to Russia's energy security. *Voprosy kiberbezopasnosti*. 2016;4:2-10. (In Russ.).
- Mussel AG, Guskova DA. Methods and approaches to ensuring cybersecurity of digital energy facilities. *Energeticheskaya politika*. 2018;5:62-72. (In Russ.).
- Muzychenko GE, Muzychenko V, Muzychenko VV. Application of the Internet of Things (IoT) in the energy sector. In: *Energy: Management, quality and efficiency of energy resources use. Proceedings of the 10th All-Russian Scientific and Technical Conference with International participation*. Blagoveshchensk; 2022. P. 286–290. (In Russ.).
- Osak AB, Panasetsky DA, Buzina EYa. The impact of cybersecurity of electric power facilities on the reliability of EES operation. In: *Methodological issues of energy system reliability research. Proceedings of the International Scientific seminar named after Y.N. Rudenko*. Issue 67. Syktyvkar; 2016. P. 377–385. (In Russ.).
- Panin DN, Bobkov EO, Balashov EA. Analysis of cyber attacks on critical information infrastructure with IoT technologies. *Avtonomiya lichnosti*. 2020;2:55-64. (In Russ.).
- Pashchenko IN, Vasiliev VI, Guzairov MB. Information protection in Smart Grid networks based on intelligent technologies: designing a rule base. *Izvestiya SFU. Tekhnicheskie nauki*. 2015;5:28-37. (In Russ.).
- Pashchenko IN, Vasiliev VI. Development of requirements for the information security system in the Smart Grid intelligent network based on ISO/IEC 27001 and 27005 standards. *Izvestiya SFU. Tekhnicheskie nauki*. 2013;12:117-126. (In Russ.).
- Petukhov AN, Gustin SYu. The reference model of security of critical information infrastructures. In: *International Conference on Soft Computing and Measurements*. St. Petersburg: St. Petersburg State Electrical Engineering LETI University after V.I. Ulyanov (Lenin); 2019. Vol 1. P. 243–246. (In Russ.).
- Petukhov AN, How to protect production from cyber threats. *Daydzhest «Neftegaz»*. 2020;17:14-17. (In Russ.).
- Verigo AA, Tsapko GP, Katashev AS. Vulnerability assessment of automated process control systems. *Mezhdunarodnyy nauchno-issledovatel'skiy zhurnal*. 2016;11-4:47-48. (In Russ.).
- Yaremchuk S. SCADA security. *Sistemnyy administrator*. 2013;6:44-47. (In Russ.).
- Zaedinov V. Prospects and challenges of the digital transformation of the Russian energy sector: From optimization to the Internet of Energy. In: *Global challenges and national environmental interests: Economic and social aspects. Proceedings of the 17th International Scientific and Practical Conference of the Russian Society for Ecological Economics (ROEE/RSEE-2023)*. Novosibirsk: IEOPP SO RAN; 2023. P. 235–240. (In Russ.).

ИНФОРМАЦИЯ ОБ АВТОРЕ

Кисленко Сергей Леонидович, кандидат юридических наук, доцент, доцент кафедры криминалистики Московского государственного юридического университета имени О.Е. Кутафина (МГЮА)
д. 9, Садовая-Кудринская ул., г. Москва 125993, Российская Федерация
ser-kislenko@yandex.ru

INFORMATION ABOUT THE AUTHOR

Sergey L. Kislenko, Cand. Sci. (Law), Associate Professor, Associate Professor, Department of Criminology, Kutafin Moscow State Law University (MSAL), Moscow, Russian Federation
ser-kislenko@yandex.ru

Материал поступил в редакцию 22 ноября 2024 г.

Статья получена после рецензирования 27 декабря 2024 г.

Принята к печати 15 августа 2025 г.

Received 22.11.2024.

Revised 27.12.2024.

Accepted 15.08.2025.