***Потенциал трансформации комплексной безопасности топливно-энергетического комплекса России в свете эволюции трансграничных угроз***

***Соколова О.М.***

*Российский государственный университет нефти и газа (НИУ) имени И. М. Губкина, Факультет комплексной безопасности ТЭК, Студент (бакалавр), 2027*

*E–mail: ovsokolova19042005@mail.ru*

В настоящее время мы живем в эпоху насыщенной изменениями реальности, как геополитической, так и экономической [1]. Можно с уверенностью заявить, что наступил момент формирования новых стратегических целей России, в частности, в области энергетики и обеспечения безопасности ТЭК страны, в свете вызовов, с которыми сталкивается российская энергетика (смещение центра мирового экономического роста в страны Азиатсво-Тихоокеанского региона; снижение мирового спроса на энергоресурсы, усиление конкуренции, изменение международного законодательства) [2]. Для предприятий ТЭК существует множество (в части принадлежности к различным сферам – информационной, технологической, антитеррористической, соци- альной и т. п.) причин возникновения инциденов, которые, в свою очередь, могут вызвать множество негативных последствий. Это, в свою очередь, порождает неделимое объединение угроз и последствий их реализации.

Такой подход принципиально отличается от имевшейся ранее точки зрения, что, например, угрозы информационной безопасности порождали негативные последствия только в сфере информационной безопасности. В настоящее время это единый "гордиев узел безопасности", что и делает последнюю комплексной.

В ходе проведенного исследования был взят широкий кластер кейсов, представляющий наиболее полную репрезентативность. Были также проанализированы две наиболее серьезные трансграничные угрозы ТЭК – энергетический терроризм и киберугрозы.

В ходе исследования были сделаны следующие промежуточные выводы:

Энергетический терроризм – явление многопрофильное. Он может преследовать как разные цели, так и иметь разные масштабы и участников. Энергетические объекты являются привлекательной и уязвимой целью террористов из-за трех особенносей: низкой мобильности и высокой концентрации, высокой стратегической и экономической ценности и географической удаленности.

В первую очередь, исполнителями террористических актов, целью которых являются объекты ТЭК определенной страны, могут быть: Государственные акторы (подрыв «Северных потоков»); Террористические организации, зачастую следующие радикальной исламистской повестке (концепция «энергетического джихада») [3]; Нерегулярные вооруженные формирования (диверсии Движения за освобождение дельты реки Нигер на нефтепроводе, принадлежащем Shell, в 2009 году); Повстанцы (взрыв повстанцами из Армии национального освобождения магистрального нефтепровода Transandino, принадлежащего компании Ecopetrol в Колумбии в 2016 году)[4]; Прочие милитаризованные организации.

В зависимости от участников терактов, цели тоже могут варьироваться: Нанесение ущерба экономическим основам страны, которые поддерживают ее политическую, военную или коммерческую мощь, что, в свою очередь угрожает национальной безопасности страны; Нанесение ущерба транснациональным кампаниям (в данном случае энергетические террористы выступают против добычи нефти на территории страны иностранными компаниями); Выбор символических целей для того, чтобы побудить людей присоединиться к их организации; Демонстрация филиалами крупных террористических групп своей поддержки и лояльности; Сбор средств (нападая на объекты ТЭК, беря в заложники работников отрасли или воруя нефть, террористы вымогают средства на финансирование своей деятельности) [5].

Масштабы угрозы также могут различаться. Можно выделить одиночные теракты и малые кампании. Применительно к России, целесообразно рассматривать именно первый вариант, особенно в свете диверсий на газопроводах «Северный поток» и «Северный поток-2», которые можно расценивать как акт энергетического терроризма.

Стремительное развитие цифровизации не обошло и энергетический комплекс. Несмотря на то, что он является критически важной отраслью для любой страны и его безопасности уделяется должное внимание, он остается одним из самых уязвимых секторов для кибератак [6]. Это связано с тем, что энергетическая отрасль довольно медленно обновляет инфраструктуру и программное обеспечение, что играет на руку хакерам. Сегодня из-за нестабильной геополитической ситуации российская энергетика становится более уязвимой для зарубежных хакеров. По разным оценкам, отечественный энергетический сектор использует от 40 до 50 процентов иностранного ПО, а также иностранное оборудование [7]. Одним из наиболее эффективных решений для снижения риска хакерских атак извне является отказ от иностранного оборудования и ПО, а также развитие защиты.

В заключение необходимо сказать о том, что события последних лет доказали необходимость выполнения работ по антитеррористической защите объектов ТЭК и поставили перед нами новые вызовы. Необходимо корректировать нормативно-правовые акты в области антитеррористической защиты, в том числе и объектов ТЭК. Легкодоступность новых технических средств для совершения несанкционированных действий, таких как беспилотные летательные аппараты и другие, требуют ответных действий, нейтрализующих эти угрозы.

В ходе исследования был сделан вывод о том, что у РФ есть большой потенциал трансформации энергобезопасности. Чтобы сделать этот процесс наиболее эффективным, необходимо действовать в двух направлениях.

Первым направлением является деятельность в рамках страны. Помимо усиления защиты энергетических объектов и компаний, правительству России либо отдельным компаниям целесообразно предпринять и ряд других мер, а именно: активно интегрировать передовые технологии в комлекных системах безопасности (искусственный интеллект, беспроводная связь, технологии дополненной визуальной реальности и т.д.); минимизировать воздействие производства энергии на местное сообщество (например, частичный найм местных жителей и взаимодействие с обществом позволит минимизировать напряженность в богатых нефтью регионах); подготавливать высококвалифицированных специалистов в области комплексной безопасности объектов ТЭК (в том числе в рамках Антитеррористического центра государств – участников СНГ и других организаций, а также посредством проведения комплексных учений по предотвращению террористических атак); уделять повышенное внимание «мягкой силе», а именно участию институтов гражданского общества в формировании единого подхода к проблемам безопасности; широко применять БПЛА и другие технологии для контроля процессов производства, обнаружения утечек и т.д.

Вторым направлением является международная кооперация. Это путь к энергобезопасности не только России, но и всего мира. Одним из основных направлений является усиление партнерства в рамках международных организаций и объединений: ЕАЭС, СНГ, ШОС, а также БРИКС. Так, с 2015 года действует Рабочая группа по энергосбережению и повышению энергоэффективности, которая стала первой в рамках БРИКС постоянной платформой для обсуждения энергетической проблематики. В свете описанных выше событий также кажется целесообразным продолжать работу в рамках гармонизации законодательных норм в сфере безопасности ТЭК.

[1] Касаткин Д. Рынки нефти и газа на пороге передела // Инфотэк. 2022. URL: <https://itek.ru/analytics/rynki-nefti-i-gaza-na-poroge-peredela/> (дата обращения: 15.02.2024)

[2] Новая Доктрина энергетической безопасности. О чем она? // [Электронный ресурс]: ТАСС. 2019. URL: <https://tass.ru/ekonomika/6427822?ysclid=lsmw305nwk615699308> (дата обращения: 14.02.2024)

[3] Шумилин А. Грозит ли миру «энергетический джихад»? // Forbes. 2013. URL: <https://www.forbes.ru/mneniya-column/konkurentsiya/233490-energeticheskii-dzhihad?ysclid=lsmy8ydcp5142633382> (дата обращения: 16.02.2024)

[4] Специальный бюллетень CTN. Защита важнейших объектов энергетической инфраструктуры от террористических актов // [Электронный ресурс]: ОБСЕ. 2010. URL: <https://www.osce.org/files/f/documents/3/f/70164.pdf> (дата обращения: 15.02.2024)

[5] Понимание кибер-рисков в нефтегазовой отрасли // [Электронный ресурс]: ЭнергоСМИ. 2020. URL: <https://energosmi.ru/archives/44324> (дата обращения: 15.02.2024)

[6] Лаврухин М. Терроризм в энергетической промышленности // Энергетическая политика. 2023. URL: <https://energypolicy.ru/terrorizm-v-energeticheskoj-promyshlennosti/neft/2023/14/23/?ysclid=lsrnxrelf9500704481> (дата обращения: 14.02.2024)

[7] Мамонова Е. Сектор энергетики стал одной из основных мишеней кибератак // RG.ru. 2022. URL: <https://rg.ru/2022/05/17/sektor-energetiki-stal-odnoj-iz-osnovnyh-mishenej-kiberatak.html?ysclid=lsmx4hx5tw640760418> (дата обращения: 15.02.2024)

**Источники и литература:**

1. Указ Президента Российской Федерации от 13.05.2019 г. № 216 Об утверждении Доктрины энергетической безопасности Российской Федерации
2. *Лаврухин М.* Терроризм в энергетической промышленности // Энергетическая политика. 2023. URL: <https://energypolicy.ru/terrorizm-v-energeticheskoj-promyshlennosti/neft/2023/14/23/?ysclid=lsrnxrelf9500704481> (дата обращения: 14.02.2024)
3. *Мамонова Е*. Сектор энергетики стал одной из основных мишеней кибератак // RG.ru. 2022. URL: <https://rg.ru/2022/05/17/sektor-energetiki-stal-odnoj-iz-osnovnyh-mishenej-kiberatak.html?ysclid=lsmx4hx5tw640760418> (дата обращения: 15.02.2024)
4. *Касаткин Д.* Рынки нефти и газа на пороге передела // Инфотэк. 2022. URL: <https://itek.ru/analytics/rynki-nefti-i-gaza-na-poroge-peredela/> (дата обращения: 15.02.2024)
5. *Шумилин А.* Грозит ли миру «энергетический джихад»? // Forbes. 2013. URL: <https://www.forbes.ru/mneniya-column/konkurentsiya/233490-energeticheskii-dzhihad?ysclid=lsmy8ydcp5142633382> (дата обращения: 16.02.2024)
6. Новая Доктрина энергетической безопасности. О чем она? // [Электронный ресурс]: ТАСС. 2019. URL: <https://tass.ru/ekonomika/6427822?ysclid=lsmw305nwk615699308> (дата обращения: 14.02.2024)
7. Понимание кибер-рисков в нефтегазовой отрасли // [Электронный ресурс]: ЭнергоСМИ. 2020. URL: <https://energosmi.ru/archives/44324> (дата обращения: 15.02.2024)
8. Специальный бюллетень CTN. Защита важнейших объектов энергетической инфраструктуры от террористических актов // [Электронный ресурс]: ОБСЕ. 2010. URL: <https://www.osce.org/files/f/documents/3/f/70164.pdf> (дата обращения: 15.02.2024)