УДК: 004.056.5+620.9

***Массель А.Г.***

# КИБЕРАТАКИ КАК УГРОЗА ЭНЕРГЕТИЧЕСКОЙ БЕЗОПАСНОСТИ РОССИИ

**Анотація:**

*У статті акцентується увага на необхідність розширення переліку стратегічних загроз ЕБ за рахунок включення кіберзагроз. По аналогії з дослідженнями проблем ЕБ пропонується розробка превентивних , оперативних і ліквідаційних заходів, спрямованих на запобігання і/чи ліквідацію наслідків як порушення порушення роботи ІТ-систем, так і НС в енергетиці, які можуть бути наслідком успішних кібератак.*

**Аннотация:**

*В статье акцентируется внимание на необходимости расширении перечня стратегических угроз ЭБ за счет включения киберугроз. По аналогии с исследованиями проблем ЭБ предлагается разработка превентивных, оперативных и ликвидационных мероприятий, направленных на предотвращение и/или ликвидацию последствий как нарушения работы ИТ-систем, так и ЧС в энергетике, которые могут быть следствием успешных кибератак.*

**Abstract:**

*The article focuses on the need to expand the list of strategic threats DL to include cyber threats.The development of preventive, operational and liquidation activities aimed at preventing and / or eliminating the consequences of the IT systems breach and emergency in the energy sector, which may be the result of successful cyber attacks, are proposed by analogy with the research problems EB*

## Введение

Под энергетической безопасностью (ЭБ) России и ее регионов понимается защищенность жизненно важных энергетических интересов личности, общества и государства от внутренних и внешних угроз (бесперебойное обеспечение потребителей экономически доступными топливно-энергетическими ресурсами приемлемого качества: в нормальных условиях – обеспечение в полном объеме обоснованных потребностей, в чрезвычайных ситуациях – гарантированное обеспечение минимально необходимого объема важных потребностей) [1]. До последнего времени при рассмотрении угроз ЭБ не рассматривались проблемы кибербезопасности, которые усугубляются тенденциями распространения в России концепции Smart Grid, подразумевающей интеграцию усовершенствованной технологической инфраструктуры и современных информационных технологий. Автор предлагает расширить перечень стратегических угроз ЭБ за счет включения киберугроз. Для моделирования киберугроз и последствий вызванных ими ЧС в энергетике предлагается использовать разработанные и применявшиеся ранее автором интеллектуальные технологии онтологического, когнитивного и событийного моделирования. Эти технологии могут быть полезны также при проведении аудита энергетических объектов с точки зрения ки-

бербезопасности, составления паспортов безопасности, разработки соответствующих методик и инструкций.

**Угрозы энергетической безопасности.**

Вся совокупность угроз, могущих оказать влияние на работу систем энергетики, условно делится на две группы [1]. Первая группа представляет собой ординарные угрозы – достаточно вероятные отказы и аварии, которые являются предметом исследований надежности систем энергетики. Для компенсации таких возмущений в системах энергетики предусматриваются различные формы резервирования мощностей по производству и транспортировке ТЭР, структурных решений по обеспечению гарантированного энергоснабжения отдельных категорий потребителей, включая создание соответствующих запасов ТЭР. При нормальных условиях развития и функционирования национальной экономики такие негативные явления не всегда угрожают энергетической безопасности государства, тогда как на фоне неординарных воздействий на энергетику они способны в значительной степени усугубить ситуацию.

Опасными для ЭБ являются угрозы, входящие во вторую группу. Это различные неординарные явления, которые уникальны по причинам возникновения, характеру развития и последствиям. Конкретные угрозы для энергетической безопасности России имеют социально-политические, экономические, техногенные и природные причины. Отдельную группу составляют внешнеполитические и внешнеэкономические угрозы. По причинам возникновения такие угрозы ЭБ классифицируются на природные, техногенные, экономические, социально - политические и управленческие.

Последствия реализации угроз ЭБ многогранны и разнообразны. Разные виды угроз характеризуются различными поражающими факторами и поражаемыми объектами, и могут приводить к различным последствиям.

Среди этих угроз до последнего времени не рассматривались угрозы кибербезопасности, которые на самом деле могут спровоцировать как проблемы обеспеченности энергоресурсами, так и чрезвычайные ситуации в энергетике. Необходимость рассмотрения в составе угроз ЭБ киберугроз усугубляется также тенденциями распространения в России концепции Smart Grid, подразумевающей интеграцию усовершенствованной технологической инфраструктуры и современных информационных технологий. К сожалению, энергетики не всегда осознают, что использование новейших технологий – это новые риски.

Рассмотрим далее понятия киберугроз, кибератак и возможные негативных последствия их реализации с позиций энергетической безопасности.

**Кибератака, атака из киберпространства** (cyber attack) – атака, проводимая с помощью программных и аппаратных средств на компьютерные сети и компьютерные системы противника.

Другое определение: кибератака - это намеренные попытки изменить, нарушить или остановить функционирование компьютерных систем или сетей, а также программ или информации, которые они содержат или передают [2].

Говоря о кибератаках, следует иметь ввиду, что, помимо умышленных действий, вред могут причинить действия неумышленные (можно назвать их киберхалатностью), обусловленные, например, низкой компьютерной грамотностью или пренебрежением мерами, обеспечивающими кибербезопасность, которые по причиняемому ущербу сравнимы с кибератаками.

Можно привести следующую классификацию киберугроз:

1) по природе происхождения (предумышленные и непредумышленные);

2) по направлению осуществления (внешние и внутренние);

3) по объекту воздействия (АРМы пользователей и администраторов, средства документирования и отображения, каналы связи и т.д.);

4) по способу осуществления (информационные, программно - аппаратные, физические, радиоэлектронные, организационно-правовые и т.д.);

5) по жизненному циклу (разработка, ввод в эксплуатацию, эксплуатация, вывод из эксплуатации) [3].

На рис. 1 приведена онтология кибератак, которые могут быть направлены как на объекты генерации энергоресурсов, так и на объекты их транспортировки и потребления. Наиболее уязвимым звеном являются системы управления и диспетчеризации электроэнергетических систем (ЭЭС), причем уязвимость систем управления будет возрастать по мере распространения декларируемого в концепции Smart Grid в России мультиагентного подхода [4].

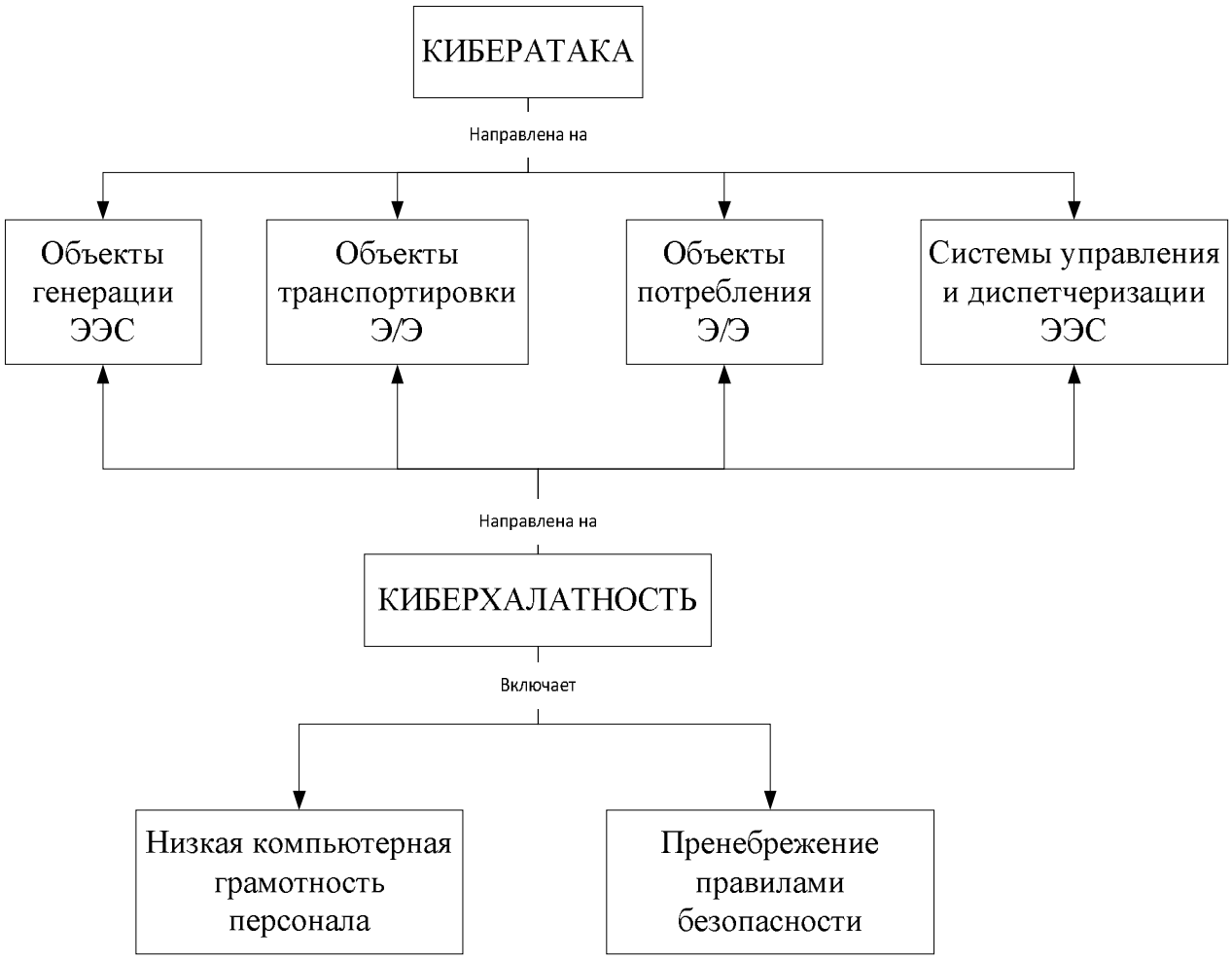


**Рис. 1 Онтология кибератак**

При исследовании киберугроз и их возможного влияния на снижение уровня ЭБ может быть применен подход, разрабатываемый для анализа стратегических угроз ЭБ, возникновения и развития ЧС в энергетике.

## Деятельность по обеспечению энергетической безопасности в период экстремальных ситуаций.

Под экстремальными ситуациями (ЭкС) понимаются как чрезвычайные, так и критические ситуации, определение которых базируется на оценке состояний систем или объектов по шкале: «норма», «предкризис» – критическая ситуация, «кризис» – чрезвычайная ситуация. Исходя из этого, под критическими ситуациями понимаются ситуации, когда возникают угрозы бесперебойному функционированию технических объектов и объектов обеспечения жизнедеятельности и/или угрозы жизни или здоровью, как отдельных людей, так и социальных (профессиональных) групп. Эти угрозы могут быть устранены принятием соответствующих превентивных и оперативных мер, которые не позволят критической ситуации (КС) перерасти в чрезвычайную ситуацию (ЧС).

Выделяются три вида мероприятий по обеспечению энергетической безопасности, которые разделяются по характеру, месту и времени применения: 1) превентивные; 2) оперативные; 3) ликвидационные [1].

*Превентивные мероприятия* в энергетическом хозяйстве по обеспечению энергетической безопасности осуществляются для снижения: возможности возникновения и реализации угроз энергетической безопасности (в том числе киберугроз); восприимчивости ТЭК и входящих в него систем топливо- и энергоснабжения к различного рода угрозам.

Эффект действия этих мер проявляется в снижении уровня соответствующих угроз ЭБ и, как следствие, в снижении последствий от различного рода возмущений для ТЭК, СЭ и потребителей. Выбор таких мер (с учетом уровня их экономической эффективности) может быть осуществлен на основе комплексной оценки состояния ТЭК, СЭ и положения дел с энергосбережением у потребителей. В связи с этим указанные меры должны осуществляться по следующим основным направлениям:

1. Совершенствование структуры ТЭК и систем энергетики с позиций ЭБ. Проведение мероприятий этой группы позволит уменьшить зависимость потребителей топлива и энергии от условий функционирования ТЭК и СЭ (зависимость от источников, от надежности протяженных коммуникаций).

2. Разработка и внедрение нового оборудования и технических усовершенствований в интересах ЭБ. Мероприятия второй группы осуществляются с целью повышения надежности функционирования оборудования систем энергетики, а также его лучшего соответствия требованиям реализации мер первой группы.

3. Производственно-технические мероприятия по повышению готовности систем энергоснабжения к работе в критических ситуациях с максимально возможным снижением ущерба от них для потребителей. Мероприятия третьей группы позволят компенсировать возможные недопоставки топливно-энергетических ресурсов в результате каких-либо отклонений от нормальных условий топливоснабжения.

4. Различного рода деятельность потребителей ТЭР по сокращению спроса и более эффективному использованию, по повышению гибкости потребительских энергоустановок в отношении качества и параметров энергоносителей. К четвертой группе можно отнести меры по энергосбережению и меры по возможному повышению гибкости потребительских установок, что достаточно специфично для каждой области производства.

5. Деятельность, направленная на повышение уровня киберзащищенности как систем управления ТЭК И СЭ, так и используемых ИТ-систем.

Направления 1–4 традиционно используются при анализе угроз ЭБ, пятое направление предлагается добавить в связи с необходимостью учета киберугроз.

Следующие два вида мероприятий относятся к мероприятиям, проводимым в период ЧС для выхода из них.

*Оперативные мероприятия,* заключающие в себе ограничение потребителей ТЭР, либо же отпуск ТЭР из государственных запасов.

*Ликвидационные мероприятия***.** Меры по ликвидации последствий ЧСЭ включают три группы: производственно-технические и экономические меры в сфере энергоснабжения; то же в сфере энергопотребления; меры в социальной, политической и общеэкономической сфере.

Меры второй группы весьма специфичны для каждой отрасли экономики, каждой категории потребителей, мы их касаться не будем. Не будем рассматривать и меры третьей группы ввиду их определенной универсальности, инвариантности относительно разных сфер безопасности.

На рис. 2 представлена общая схема исследований проблем ЭБ, или, иначе, оценки состояния ТЭК в условиях возможных сценариев угроз ЭБ с учетом мероприятий, направленных на повышение уровня ЭБ, которая может быть расширена в случае учета киберугроз.

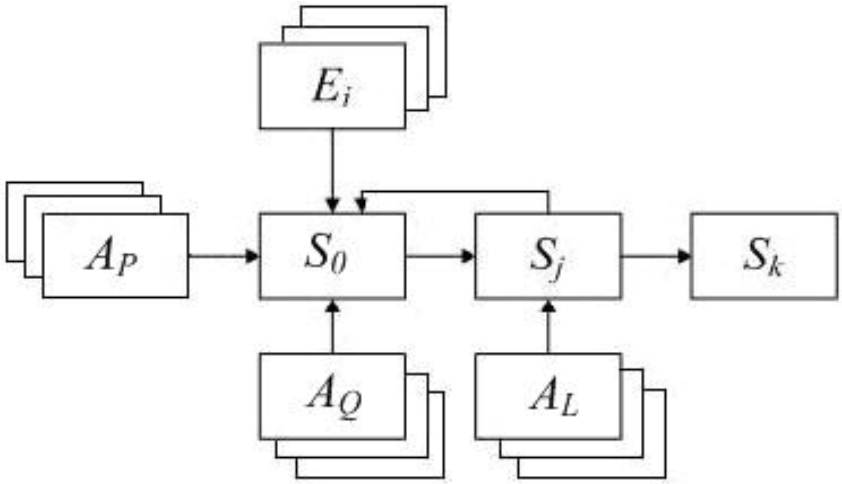


**Рис. 2 Общая схема исследований по оценке состояния ТЭК**

Здесь $S_0$ – начальное состояние ТЭК; $E_i$ – сценарий возможной чрезвычайной ситуации, возникающей в случае реализации как угроз ЭБ, так и киберугроз; $A = A_P \cup A_Q \cup A_L$ – набор превентивных, оперативных и ликвидационных мероприятий, предотвращающих, нейтрализующих или смягчающих последствия чрезвычайной ситуации; $S_j$ – состояние ТЭК после чрезвычайной ситуации $E_i$ (реализации угроз) с учетом выполнения набора мероприятий $A_P$ и/или $A_Q$; $S_k$ – состояние ТЭК после проведения ликвидационных мер $A_L$.

Основная цель вычислительного эксперимента в исследованиях, схематически показанных на рис. 2 – определение инвариантного набора мероприятий $A = A_P \cup A_Q \cup A_L$, выполнение которых в условиях нормального функционирования

позволит минимизировать и/или предотвратить вовсе последствия наибольшего числа возможных чрезвычайных ситуаций.

При учете киберугроз этот набор мероприятий должен быть дополнен специфическими мероприятиями, направленными на предотвращение киберугроз, отражение кибератак и/или ликвидацию последствий кибервторжений. Необходимо учитывать, что требуется комплексное решение проблемы, так как в случае успешной кибератаки придется ликвидировать последствия не только самой кибератаки (нарушение работы ИТ-систем), но и возможных ЧС в энергетике, вызванные сбоями в работе этих систем.

Очевидно, что для определения инвариантного набора мероприятий $A = A_P \cup A_O \cup A_L$ необходимо моделирование возможных кибератак и их последствий. Для этого предлагается использовать интеллектуальные технологии, применявшиеся коллективом, который представляет автор, для анализа угроз ЭБ и развития возможных ЧС в энергетике [5].

**Интеллектуальные технологии, предлагаемые для моделирования и анализа последствий киберугроз.**

Предлагается использовать для этих целей онтологическое, когнитивное и событийное моделирование. Их сравнение приведено в табл. 1.

Подробно эти технологии с примерами их применения описаны в работах [6–8]. Имеются реализации протипов инструментальных средств для поддержки этих видов моделирования (OntoMap, CogMap, EventMap). Применительно к поставленной проблеме эти технологии, помимо моделирования киберугроз и кибератак, могут быть полезны при проведении аудита энергетических объектов с точки зрения кибербезопасности, составления паспортов безопасности, соответствующих методик и инструкций.

Таблица 1

**Сравнение технологий онтологического,когнитивного и событийного моделирования**

| Технология | Назначение | Аппарат для формализованного представления | Использование в исследованиях энергетической безопасности |
|---|---|---|---|
| Онтологическое моделирование | Для описания декларативных фрагментов знаний | Онтологии (Специальные языки (OWL, RDF, XML и др.)) | Для выявления, классификации и спецификации концептов (основных понятий в исследованиях энергетики, в т.ч. связанных с кибербезопасностью) |
| Когнитивное моделирование | Для выявления причинно–следственных связей концептов | Когнитивные карты (теория графов) | Для анализа угроз ЭБ, в т.ч. киберугроз |
| Событийное моделирование | Построение поведенческих моделей. Выявление динамики развития ЧС | Событийные карты (теория Joiner-сетей) | Для анализа развития и последствий ЧС, в т.ч. вызванных реализацией кибератак |

## Заключение

В статье акцентируется внимание на необходимости расширения перечня стратегических угроз ЭБ за счет включения киберугроз. По аналогии с исследованиями проблем ЭБ предлагается разработка превентивных, оперативных и ликвидационных мероприятий, направленных на предотвращение и/или ликвидацию последствий как нарушения работы ИТ-систем, так и ЧС в энергетике, которые могут быть следствием успешных кибератак. Для моделирования киберугроз и развития ЧС в энергетике, вызванных кибервторжениями, предлагается использовать интеллектуальные технологии: онтологическое, когнитивное и событийное моделирование и поддерживающие их инструментальные средства.

Результаты, представленные в статье, получены при частичной финансовой поддержке грантов интеграционных проектов СО РАН №145, СО РАН и НАН Беларуси №18, гранта Программы Президиума РАН №229 и грантов РФФИ №13-07-00140 и №13-07-00359.

**Литература:**

1. Бушуев В.В. Энергетическая безопасность России / В.В. Бушуев, Н.И. Воропай, А.М. Мастепанов, Ю.К. Шафраник и др. – Новосибирск: Наука, 1998.–302 с.

2. Понимание киберпреступности: Руководство для развивающихся стран. Проект. [Электронный ресурс]. – Режим доступа: http://www.itu.int/dms_pub/itu-d/oth/01/0B/D010B0000073301PDFR.pdf. – Название с титул. экрана.

3. Гайдамакин Н.А. Теоретические основы компьютерной безопасности / Н.А. Гайдамакин – Екатеринбург: Изд-во Уральского университета, 2008. – 212 с.

4. Кобец Б.Б. Инновационное развитие электроэнергетики на базе концепции Smart Grid / Б.Б. Кобец, И.О. Волкова. – М.: ИАЦ Энергия, 2010. – 208 с.

5. Массель А.Г. Интеллектуальная ИТ-среда для исследований проблемы энергетической безопасности / А.Г. Массель // Труды Международной конференции «Информационные технологии в науке, образовании, телекоммуникации и бизнесе». Приложение к журналу «Открытое образование». – Гурзуф, 2010. – С. 306–309.

6. Копайгородский А.Н. Применение онтологий при построении информационной инфраструктуры исследований в энергетике / А.Н. Копайгородский // Сборник трудов Всероссийской конференции «Инженерия знаний и технологии Semantic Web – 2011». – СПб: НИУ ИТМО, 2011. – С. 127–136.

7. Массель А.Г. Когнитивное моделирование угроз энергетической безопасности / А.Г. Массель // Горный информационно-аналитический бюллетень (научно-технический журнал). – 2010. – № 17. – С. 194–199.

8. Аршинский В.Л. Событийное моделирование чрезвычайных ситуаций в энергетике / В.Л. Аршинский // Труды Международной конференции «Информационные технологии в науке, образовании, телекоммуникации и бизнесе». Приложение к журналу «Открытое образование». – Гурзуф, 2010. – С. 299–301.