Литература:

1. *Шульц В.Л., Кульба В.В., Шелков А.Б., Чернов И.В.* Сценарный анализ в управлении геополитическим информационным противоборством. – М.: Наука, 2015. – 542 с.

2. *Дранко О.И., Новиков Д.А., Райков А.Н., Чернов И.В.* Управление развитием региона. Моделирование возможностей. – М.: URSS, ООО «ЛЕНАНД», 2023. – 432 с.

3. *Информационное* обеспечение систем организационного управления (теоретические основы). В 3-х частях. / Под ред. Е.А. Микрина, В.В. Кульбы. – М.: Изд-во физико-математической литературы, 2012. Ч. 3. – 528 с.

4. *Чернов И.В.* Сценарно-когнитивное моделирование сложных систем на основе событийной идентификации динамики факторов // Проблемы управления. – 2023. – № 3. – С. 65-76.

Михалевич И.Ф., Франсишко Нелсон А.М.

Моделирование угроз безопасности объектов критической информационной инфраструктуры Республики Ангола

Аннотация: В статье рассматривается процесс построения модели угроз для объектов электроэнергетики критической информационной инфраструктуры Республики Ангола. Проведен анализ ключевых активов, определены основные уязвимости и потенциальные злоумышленники. Представлена модель угроз, учитывающая специфику национальной энергосистемы, ее географические и технологические особенности. Результаты исследования могут быть использованы регуляторами и операторами объектов электроэнергетики КИИ Анголы для разработки эффективных мер по защите от компьютерных атак и обеспечения устойчивой работы объектов.

Ключевые слова: автоматизированная система, защита информации, компьютерная атака, компьютерная безопасность, критическая информационная инфраструктура, информационная система, модель угроз,

нормативно-правовое регулирование безопасности критической информационной инфраструктуры, электроэнергетика, Республика Ангола

Введение

Критическая информационная инфраструктура (КИИ) включает в себя объекты обработки информации, нарушение безопасности которой может повлечь тяжелые последствия для страны во многих чувствительных сферах [1], включая электроэнергетику. Современные энергетические системы Республики Ангола представляют собой интегрированные автоматизированные системы корпоративного и технологического управления, в которых процессы генерации, передачи и распределения электроэнергии неразрывно связаны с цифровыми технологиями [2, 3]. Их применение повышает эффективность функционирования объектов, но одновременно расширяет возможности нарушителей информационной безопасности для совершения компьютерных атак [4], что требует применения в КИИ доверенных решений [1, 5].

Энергетический сектор Республики Ангола сталкивается с новыми вызовами в области информационной (компьютерной) безопасности [6], что требует актуализации моделей угроз. Моделирование угроз представляет собой описание потенциальных угроз, нарушителей безопасности объектов КИИ, рисков и неблагоприятных последствий, в случае реализации угроз [7]. Модель угроз позволяет систематизировать знания о возможных источниках и способах реализации компьютерных атак, оценить возможные риски и выработать решения для нейтрализации угроз [8].

1. Типовые объекты электроэнергетики КИИ Анголы

Типовыми объектами электроэнергетики КИИ Республики Ангола являются:

– центры управления энергосистемой (ЦУС). Это ключевые узлы, осуществляющие диспетчеризацию и балансировку энергосети в масштабах страны или региона;

– объекты генерации электроэнергии. Это ГЭС (например, каскад ГЭС на реке Кванза, включая ГЭС Лаука) и тепловые электростанции;

– линии электропередач (ЛЭП) и высоковольтные подстанции. Они связывают регионы и являются узловыми точками энергетической системы страны;

– SCADA и АСУ ТП, управляющие технологическими процессами на всех уровнях выработки, доставки и распределения электроэнергии;

– информационные системы. Это системы биллинга, учета энергопотребления, CRM и ERP-системы энергокомпаний (например, Empresa Nacional de Electricidade – ENE).

Спецификой ангольской энергосистемы является относительно слабая разветвленность и высокая концентрация объектов генерирации. Это делает ее уязвимой к каскадным авариям, которые могут быть спровоцированы компьютерной атакой на отдельную подстанцию или линию.

Масштабная цифровизация зачастую приводит к интеграции систем корпоративного и технологического управления объектов КИИ, что необходимо учитывать при разработке моделей угроз [5].

2. Источники угроз и потенциальные нарушители

В соответствии с применимой методологией регуляторов в сфере безопасности КИИ Российской Федерации модель угроз безопасности объектов КИИ Республики Ангола предусматривает два типа и четыре вида возможных нарушителей. К первому типу относятся внешние, ко второму – внутренние нарушители. Вид нарушителя определяют его потенциальные возможности. Соответственно выделяют нарушителей, обладающих базовыми, базовыми повышенными, средними и высокими возможностями (потенциалом). При этом учитывается мотивация потенциальных нарушителей: от мести уволенных работников, козней конкурентов, финансового обогащения, до причинения ущерба государственным (национальным) интересам. Последнее реализуется силами APT-группировок (APT – Advanced Persistent Threat), спонсируемых, как правило правительствами заинтересованных стран.

Типичные сценарии атак являются DDoS-атаки на сайты государственных, коммерческих организаций, внедрение вредоносного программного обеспечения в автоматизированные системы корпоративного и технологического управления, перехват управления распределительными узлами, нарушение передачи

телеметрических данных, атаки на цепочки поставок и эксплуатация уязвимостей [1, 5, 7, 9, 10].

3. Модель угроз типовых объектов электроэнергетики КИИ Республики Ангола

Основные элементы модели угроз типовых объектов электроэнергетики КИИ Анголы приведены в таблице 1 по векторам атак представлен на таблице 1.

Таблица 1 – Модель угроз объектов электроэнергетики КИИ Анголы (фрагмент)

Угроза	Типовые объекты воздействия	Последствия реализации атак
Внедрение вредоносного ПО (Ransomware, Wiper)	Рабочие станции сотрудников, серверы учетных данных, ERP-систем, …	Шифрование данных, останов биллинга, финансовых операций, офисных приложений, …
Атаки на АСУ ТП/SCADA	Человеко-машинный интерфейс, программируемые логические контроллеры, каналы связи между объектами, …	Несанкционированное отключение генераторов, переключение режимов работы подстанций, вывод оборудования из строя, веерные отключения, …
DDoS-атаки	Каналы связи ЦУС, внешние интерфейсы для потребителей, сайты, …	Нарушение связи между объектами, невозможность удаленного управления, отказ в обслуживании
Фишинг и целевые атаки на персонал (Spear Phishing)	Сотрудники с доступом к информационным ресурсам объектов КИИ (инженеры, IT-администраторы)	Кража учетных данных, получение первоначального доступа в сеть для последующей эскалации привилегий, …
Кража конфиденциальных данных	Базы данных потребителей, проектная документация, схемы сетей, …	Финансовые потери, шантаж, получение конкурентных преимуществ,

		подготовка к более сложным атакам
Компрометация цепочек поставок	Оборудование и ПО сторонних производителей, подрядчики	Внедрение закладок в оборудование на этапе производства, атаки через системы обновления ПО
Человеческий фактор и ошибки конфигурации	Неправильно сконфигурированное сетевое оборудование, системы защиты	Создание «лазеек» для внешних атакующих, непреднамеренные сбои в работе систем

4. Рекомендации по противодействию угрозам

Основными рекомендациями по повышению защищенности объектов энергетики КИИ Республики Ангола являются следующие:

Сегментация сетей. Она предполагает строгое разделение подсистем корпоративного и технологического управления, создание демилитаризованных зон, разделение потоков данных средствами межсетевого экранирования.

Регулярное обновление ПО безопасности и исправление ошибок, управление этими процессами, в том числе путем нормативно-правового регулирования (регламентации).

Многофакторная аутентификация (MFA) как обязательное условие для доступа ко всем критически важным системам, включая инженерные станции.

Повышение осведомленности персонала: регулярный тренинг сотрудников по выявлению фишинговых писем и иных признаков социальной инженерии.

Создание центров оперативного обнаружения и реагирования на компьютерные атаки и инциденты компьютерной безопасности в секторе электроэнергетики.

Регулярное резервное копирование информации план восстановления и отработка процедур восстановления после компьютерных атак.

Совершенствование нормативной-правовой базы обеспечения безопасности КИИ Республики Ангола, с принятием национального закона, аналогичного российскому ФЗ-187 2017 года. Это обяжет руководство государственных и коммерческих организаций

объектов КИИ выполнять минимальные требования по безопасности.

Создание национального центра обнаружения компьютерных атак и реагирования на инциденты компьютерной безопасности.

Развитие международного сотрудничества в области компьютерной безопасности (например, через Африканский союз или ITU).

Заключение

Цифровая трансформация сектора электроэнергетики Республики Ангола несет в себе как огромные возможности, так и серьезные вызовы в области компьютерной безопасности. Представленная модель угроз безопасности учитывает специфику энергосистемы страны, ее географические и технологические особенности. Результаты исследования могут быть использованы регуляторами и операторами объектов электроэнергетики КИИ Анголы для разработки эффективных мер по защите от компьютерных атак и обеспечения устойчивой работы объектов.

Литература:

1. *Михалевич И.Ф.* Методологические основы создания национальных защищенных аппаратно-программных платформ для критических информационных инфраструктур // T-Comm: Телекоммуникации и транспорт. – 2018. – Т. 12, № 3. – С. 75-81. – DOI: 10.24411/2072-8735-2018-10056.

2. *Venkatachary S.K., Alagappan A. & Andrews L.J.B.* Cybersecurity challenges in energy sector (virtual power plants) – can edge computing principles be applied to enhance security? // Energy Inform. – 2021. – Vol. 4. – Article number: 5. – URL: https://doi.org/10.1186/s42162-021-00139-7 (дата обращения 1.09.2025).

3. *Saqib Saeed, Hina Gull, Muneera Mohammad Aldossary* Digital Transformation in Energy Sector: Cybersecurity Challenges and Implications // MDPI. – 2024. – №15*(*12). – 764. – DOI: 10.3390/INFO15120764.

4. *Andrey O. Kalashnikov, Igor F. Mikhalevich.* About the single system of protection classes elements of critical information infrastructure by the criteria of importance and information security. International

Journal of Engineering & Technology. – 2018. – Vol.7 (2.23). – P. 247-250. – DOI: 10.14419/ijet.v7i2.23.11952.

5. *Баранов Л.А., Михалевич И.Ф.* О доверии к системам автономного судоходства критической информационной инфраструктуры // T-Comm: Телекоммуникации и транспорт. – 2025. – Том 19, №6. – С. 52-59. – DOI: 10.36724/2072-8735-2025-19-6-52-59.

6. *Франсишко, Н.А.М.* Анализ особенностей обеспечения безопасности критической информационной инфраструктуры Республики Ангола // REDS: Телекоммуникационные устройства и системы. – 2025. – Т. 15, № 2. – С. 18-22.

7. *Ismail Zaky Al Fatih, Arthur Josias Simon Runturambi, Stepi Anriani.* The Impact of Cyberattacks on Jakarta's Electric Energy Sector: An Evaluation of Risk, Security, and Economic Implications // Journal of Social Science. – 2024. – Volume 3. Number 11. – DOI: 10.57185/JOSS.V3I11.378.

8. *Чернов Д.В., Сычугов А.А.* Формализованное представление модели угроз информационной безопасности АСУ ТП // Радиотехника. – 2019. – Т. 83, № 6(7). – С. 74-80. – DOI: 10.18127/j00338486-201906(7)-13.

9. *Грюнталь А.И., Базаева С.Е.* Вопросы обеспечения кибербезопасности при разработке и использовании АСУ ТП / Труды научно-исследовательского института системных исследований Российской академии наук. – 2021. – Т. 11, № 4. – С. 56-67. – DOI: 10.25682/NIISI.2021.4.0006.

10. *Попов П.А., Розенберг Е.Н., Сабанов А.Г., Шубинский И.Б.* Концепции обеспечения комплексной безопасности АСУ ТП верхнего уровня управления для объектов КИИ железнодорожного транспорта // Надежность. – 2025. – № 25(3) – С. 42-49. – URL: https://doi.org/10.21683/1729-2646-2025-25-3-42-49 (дата обращения 1.09.2025).

Фуругян М.Г.

Управление комплексом работ с периодически поступающими заявками

Аннотация: Рассматривается задача управления комплексом работ в случае, когда заявки на выполнение каждой работы поступают периодически, начиная с