Ростелеком
Солар

Анализ нарушений работоспособности объектов электроэнергетики в результате деструктивных воздействий компьютерных атак

Отчет о научно-исследовательской работе Лаборатории кибербезопасности АСУ ТП. Издание первое. Сокращенная версия.

Для экспертов электроэнергетической отрасли

Executive Summary

На сегодняшний день цифровизация экономики является одной из главных целей экономического и технологического развития Российской Федерации. Одна из приоритетных задач цифровизации экономики – цифровизация электроэнергетической отрасли.

По расчетам цифровизация электроэнергетического сектора обеспечит большие преимущества:

- увеличение гибкости работы электрических сетей;
- снижение затрат;
- повышение надежности электроснабжения;

Однако положительные эффекты могут быть нивелированы или вообще не достигнуты из-за растущих вместе с цифровизацией рисков нарушений работы объектов электроэнергетики вследствие реализации киберугроз.

В настоящем отчете приведен анализ возможных нарушений работы объектов электроэнергетики с высоким уровнем цифровизации вследствие кибератак, а также возможных технологических причин таких нарушений. Приведены методики кибератак и виды киберинцидентов, к которым они могут приводить. Например, несанкционированный доступ, отказ в обслуживании, модификация (подмена) данных и т.д.

Результатами возникновения таких инцидентов или их совокупности могут быть повреждения первичного оборудования, массовые отключения потребителей, выбросы отравляющих и радиоактивных веществ, как следствие гибель людей, выход из строя инфраструктурных объектов здравоохранения, коммунального хозяйства, остановка промышленного производства и т.д.

При атаке на несколько подстанций, работающих с высокими и сверхвысокими классами напряжений, могут выводиться из строя целые областные энергосистемы, что ведет к снижению надежности и нарушению устойчивости ЕЭС России.

При этом в исследовании сознательно не делается детализация того, как конкретно должна реализовываться атака, поскольку публикация такой информации несет опасность реализации рисков нарушения энергетической безопасности Российской Федерации.

Сформулированная в настоящем отчете проблематика во многом справедлива не только для цифровых подстанций (ЦПС), но и для высокоавтоматизированных подстанций, построенных в соответствии с так называемой «переходной архитектурой», включающей в себя как элементы ЦПС, так и элементы классической инфраструктуры подстанции, и наследуемые протоколы автоматизации.

Наиболее значимым практическим результатом работы авторы считают возможность сделать следующий вывод: нарушение устойчивого функционирования объектов электроэнергетики с высоким уровнем цифровизации вторичных систем вследствие воздействия на них кибератак возможно.

Введение

Вопросам цифровой трансформации электроэнергетической отрасли в последние годы уделяется особое внимание. Сама потребность в модернизации практически не вызывает сомнений [14], [15]. Дискуссионными остаются конкретизация целей, которые необходимо будет достичь в результате трансформации отрасли, а также выбор технологической основы, на которой будет базироваться будущее российской электроэнергетики.

Было сделано несколько попыток дать качественную и количественную оценку потенциально получаемым выигрышам от цифровой трансформации. Хороший пример такой попытки – материалы конференции «Цифровая трансформация электроэнергетики России» 2017 года [14].

В рамках подготовки к конференции был сформирован образ будущего «Цифровой электроэнергетики» в 2025 году [16]. Одна из наиболее важных составляющих образа будущего описана там так: «В энергетике проведена необходимая модернизация, преодолен разрыв между скоростью старения оборудования и внедрением нового оборудования на основе цифровых технологий. Потребителям предоставляется электроэнергия по оптимальному тарифу с прогнозируемым необходимым качеством и надежностью. Создана система, готовая противостоять многообразию рисков: технологической зависимости, рисков нарушения надежного, безопасного, эффективного функционирования».

В последние годы внедрение цифровых, информационно-коммуникационных технологий на объектах электроэнергетического комплекса набирает все большие масштабы, в том числе в связи с началом реализации концепции цифровой трансформации энергетической отрасли. Существующий электроэнергетический комплекс России подлежит модернизации в целях организации единой цифровой среды технологических данных, которая позволит проводить аналитические исследования для принятия оптимальных управленческих решений, а также

анализировать информацию о состоянии оборудования, прогнозировать вероятность и последствия отказов для снижения рисков выхода оборудования из строя путем своевременного адресного ремонта или замены.

Например, ПАО «Россети» декларирует следующие цели цифровой трансформации: снижение капитальных затрат на строительство новых объектов и операционных затрат на эксплуатацию и обслуживание действующих (CAPEX и OPEX), уменьшение времени ликвидации технологических нарушений, обеспечение доступности технологических присоединений для потребителей, возрастание адаптивности системы, образование новых сервисов и моделей потребления [14], [15], [17], [18], [19].

Для получения описанных выше эффектов, как следует из концепции цифровой трансформации, будет создана цифровая электрическая сеть. Преимущества такой сети:

- Возможность управления режимами работы электрических сетей с помощью средств дистанционного управления оперативными переключениями;
- Автоматическое регулирование напряжения;
- Перераспределение нагрузки путем реконфигурации распределительной сети;
- Самодиагностика и самовосстановление после сбоев в работе отдельных элементов.

Как известно, структурной единицей цифровой электрической сети является цифровая подстанция, связанная с центром управления сетями и соседними подстанциями, которая может функционировать и эксплуатироваться без постоянного присутствия оперативного персонала [20]. Поэтому оперативное управление и мониторинг будет осуществляться из центра управления сетями.

Еще одной из разработанных концепцией развития электроэнергетики является «Интернет энергии»: построение

сетей с накопителями электроэнергии, распределенными установками малой генерации, использование возобновляемых источников энергии (ВИЭ) и цифровых интеллектуальных систем управления. Переход к новой технологической парадигме не отменяет необходимость развития и обновления большой энергетики [21]. Также реализуются концепции цифровых районных электрических сетей [22]. Преимущества такого подхода заключаются в повышении гибкости работы электрических сетей, бесперебойном электроснабжении в условиях растущего электропотребления, снижении выброса парниковых газов в атмосферу и декарбонизации энергетической отрасли.

К 2019 году в России функционирует более 5 цифровых подстанций [23] и свыше 100 тысяч реконструированных подстанций с микропроцессорными терминалами РЗА, а также АСУ ТП на основе цифровых технологий. Все больше подстанций переводится на телеуправление. До 2021 года ПАО «ФСК ЕЭС» (входит в группу «Россети») реализует дистанционное управление на 93 подстанциях по всей стране – технология уже работает на 24 подстанциях компании. К 2025 году все подстанции ФСК ЕЭС будут обеспечены цифровой связью с возможностью удаленного управления из единых центров, также будут реализованы 33 проекта цифровых подстанций с более глубокой степенью цифровизации [24].

Минэнерго России при активном участии компаний ТЭК сформировало ведомственный проект «Цифровая энергетика» [25]. «В рамках отраслевых направлений особую важность представляет цифровая трансформация электроэнергетики: она будет способствовать повышению эффективности работы организаций ТЭК, качества оказания услуг потребителям – позволит повысить надежность и качество энергоснабжения потребителей, снизить аварийность за счет внедрения риск-ориентированного подхода в управлении, сократить сроки технологического присоединения к электрическим сетям», – описано в ведомственном проекте [25]. Группа «Интер РАО», государственная корпорация «Росатом» и системный оператор ЕЭС России под эгидой Министерства энергетики РФ учредят Ассоциацию организаций цифрового развития электроэнергетики «Цифровая энергетика» [26], что указывает на участие в проекте генерирующих и сетевых

компаний. На II Международной конференции «Цифровая подстанция. Стандарт IEC 61850» АО «РАСУ» уже представляли себя как интегратор решений и центр компетенций по цифровой энергетике [27]. ПАО РусГидро на Нижегородской ГЭС создало цифровой полигон для апробации оптических и электронных ТТ и ТН, также решений по организации подсистем РЗА ЦПС в условиях опытно-промышленной эксплуатации [28].

В итоге сложность систем управления объектом возрастает, так как архитектуры становятся сложнее, информация передается с помощью цифровых протоколов и обрабатывается интеллектуальными электронными устройствами, кабельные связи образуют локальные вычислительные сети. Вследствие падает надежность управления объектом. Объекты электроэнергетической отрасли являются критическими по своей значимости, поскольку нарушение функционирования любого из них приводит к снижению надежности электроснабжения потребителей и устойчивости энергосистемы в целом. И чем выше класс рабочего напряжения оборудования и присоединений на объекте, тем большее влияние на системную надежность он оказывает.

Кибератаки – один из дестабилизирующих факторов устойчивого функционирования объекта электроэнергетической отрасли.

Возможные цели атак:

- Несанкционированный доступ к управлению коммутационной аппаратурой на подстанции, что в свою очередь может привести к массовому отключению потребителей;
- Несанкционированный доступ к данным, являющимся коммерческой тайной;
- Подмена информации, отправляемой в центр управления сетями, для невозможности расследования технологических нарушений.

Кибератаки могут приводить к нарушению работы объекта и прерыванию технологического процесса. Риски нарушения технологического процесса необходимо минимизировать, однако они возрастают с увеличением уровня цифровизации объекта, появления дополнительных сервисов, применения ПО и оборудования разных вендоров.

Границы исследования.
В данной работе исследуются сценарии кибератак на объекты электроэнергетического комплекса, целью и результатом которых могут быть реальные аварии.

Так как цифровизация подразумевает внедрение цифровых подстанций, то рассмотрению подлежат кибератаки на автоматизированные и автоматические системы ЦПС, а также их последствия. Логической границей ЦПС являются интерфейсы взаимодействия между подстанцией и центром управления сетями и интерфейсы взаимодействия с соседними подстанциями.

Источниками киберугроз могут быть:

- Антропогенные источники (антропогенные угрозы);
- Техногенные источники (техногенные угрозы);
- Стихийные источники (угрозы стихийных бедствий, иных природных явлений).

В настоящем исследовании будут рассмотрены только угрозы, создаваемые антропогенными источниками, а точнее физическими лицами, в том числе действующими от имени различных организаций.

Необходимо отметить, что внедрение цифровых подстанций затрагивает все объекты электроэнергетики, участвующие в процессах генерации, передачи и распределения электроэнергии. Поэтому электрическая часть электрических станций под управлением систем, основанных на использовании информационно-коммуникационных технологий, будет рассматриваться как ЦПС. Схема выдачи мощности электрической станции рассматривается как подстанция в совокупности с генераторным оборудованием, так как набор силового электрооборудования станций и подстанций практически одинаков и генераторы имеют электрическую связь с остальным оборудованием. Рассматриваются электроустановки переменного и постоянного тока в пределах подстанции и воздействующие на них системы управления и защиты.

Цель исследования.
Основная цель исследования – анализ возможных нарушений устойчивого функционирования ЦПС и других объектов электроэнергетики, происходящих вследствие кибератак, а также анализ технологических причин таких нарушений и анализ возможных воздействий на автоматизированные и автоматические системы управления. Кроме того, целью является и формирование инструментария, пригодного для исследования сценариев атак на ЦПС.

Задачи исследования

- Описать ЦПС для задания контекста исследования как объект электроэнергетического комплекса; оборудование и системы, обеспечивающие технологический процесс;
- Проанализировать возможные аварии объекта электроэнергетики, критически влияющие на его работу и/или работу энергосистемы и их возможные причины;
- Определить модель нарушителя и угрозы кибербезопасности цифровой подстанции;
- Классифицировать сценарии атак на ЦПС и системы, на которые они могут быть направлены;
- Описать сценарии кибератак на ЦПС с физическими последствиями.

Решение перечисленных задач даст необходимые элементы для полноценного исследования сценариев кибератак на цифровые системы управления и защиты ЦПС.

Заключение

Выводы по исследованию

Результаты исследования отражают экспертную позицию авторского коллектива. Поставленная в первой версии исследования цель достигнута за счет преимущественного использования качественных методов анализа. По мере развития исследования авторы планируют развивать используемый методический аппарат, переходя к полуколичественным и количественным методам анализа, внедряя практики организации и проведения полунатурных испытаний на базе инфраструктуры «Лаборатории кибербезопасности АСУ ТП», полнофункциональных киберучений с привлечением к участию субъектов критической информационной инфраструктуры, работающих в сфере электроэнергетики.

Наиболее значимым практическим результатом работы авторы считают возможность сделать следующий вывод: нарушение устойчивости функционирования объектов электроэнергетики с высоким уровнем цифровизации вторичных систем из-за воздействия на них кибератак возможно.

Достигнутый результат заставляет по иному воспринимать риски цифровой трансформации электроэнергетической отрасли. Обратить внимание собственников критической информационной инфраструктуры на необходимость реализации комплексного подхода к реализации задач, связанных со снижением рисков кибербезопасности.

Результатом, заслуживающим внимания, является приведенное описание объектов электроэнергетики с высоким уровнем цифровизации и вторичных систем, как объекта защиты, которое может быть использовано иными авторскими коллективами и исследователями, занимающимися проблематикой кибербезопасности ЦПС, а также вопросами надежности функционирования ЦПС.

В исследовании впервые введен ряд терминов:

- Киберфизическая система;
- Кибербезопасность;
- Угроза кибербезопасности, нарушитель кибербезопасности;
- Кибератака;
- Киберинцидент.

Необходимость введения новых терминов продиктована недостаточностью существующего понятийного аппарата. Авторы считают возможным и целесообразным использование введенных терминов для описаний ситуаций, которые отражают влияние на физический уровень неправильной (вследствие кибератак) работы систем управления.

В работе явно показано, как реализация угроз информационной безопасности (в том числе эксплуатация уязвимостей в ПО) во вторичных системах может приводить к авариям (т.е. к реализации угроз кибербезопасности объекта электроэнергетики).

Проведен анализ технологических причин, приводящих к авариям на объекте электроэнергетики. Сопоставлены аварии с их наиболее вероятными причинами. Через анализ технологических причин аварий и анализ сценариев кибератак, в результате которых злоумышленник может добиться возникновения совокупности соответствующих технологических причин, становится возможно моделировать последствия реализации киберугроз.

В настоящем исследовании задействована методология Cyber KillChain для моделирования сценариев кибератак, уникальным является результат, детализирующий последнюю стадию развития APT атаки «достижение цели»

Рассмотрены возможные последствия кибератак на вторичные подсистемы и последствия компрометации работы таких

систем с целью дальнейшего образования технологических причин, приводящих к авариям. В совокупности образуется полная картина взаимосвязи деструктивных воздействий кибератак на вторичные системы объектов электроэнергетики с высоким уровнем цифровизации и последствий на физическом уровне. Исходя из этого, можно сделать вывод, что при расследовании аварий на таких объектах необходимо также рассматривать возможные причины в области вторичных подсистем и кибератак на них.

Практическая значимость и перспективы практического развития настоящего исследования

Результаты данного исследования имеют практическую значимость для анализа угроз кибербезопасности ЦПС или любого другого объекта электроэнергетической отрасли, производящего электроэнергию или участвующего в ее передаче и распределении, с определенным уровнем цифровизации. Анализ киберугроз и сценариев кибератак является важным этапом проектирования систем защиты, так как по результатам этих этапов предъявляются требования к средствам защиты информации, организации систем мониторинга, политикам безопасности и т.д.

После проектирования необходимо проверить работоспособность заложенного для построения системы оборудования и правильность выбора мер. Доказательством пригодности средств защиты информации для реализации на их основе цифровой подстанции в киберзащищенном исполнении являются проведенные опыты в лабораторных и полевых условиях, подкрепленные экспертным анализом.

Результаты настоящего исследования лягут в основу плана по проведению полунатурных экспериментов в «Лаборатории кибербезопасности АСУ ТП» направления «Кибербезопасность АСУ ТП» компании «Ростелеком-Солар».

Список литературы

1. Правительство Российской Федерации, «Постановление от 28 октября 2009 г. N 846,» (в ред. Постановлений Правительства РФ от 05.12.2011 N 996, от 17.10.2015 N 1114, от 10.06.2016 N 525).
2. ПАО «ФСК ЕЭС» и СТО 56947007-29.240.10.248-2017, «Нормы технологического проектирования подстанций переменного тока с высшим напряжением 35-750 кВ (НТП ПС)».
3. Федеральный закон № 187 «О безопасности критической информационной инфраструктуры Российской Федерации».
4. СТАНДАРТ ОРГАНИЗАЦИИ ПАО «РОССЕТИ», «СТО 34.01-21-004-2019 «Цифровой питающий центр. Требования к технологическому проектированию цифровых подстанций напряжением 110-220 кВ и узловых цифровых подстанций напряжением 35 кВ»,» 29.03.2019.
5. ГОСТ Р ИСО/МЭК 13335-1 - 2006, «Информационная технология. МЕТОДЫ И СРЕДСТВА ОБЕСПЕЧЕНИЯ БЕЗОПАСНОСТИ. Часть 1. Концепция и модели менеджмента безопасности информационных и телекоммуникационных технологий».
6. ГОСТ Р 50922-2006, «Защита информации. Основные термины и определения».
7. Чернобровов Н.В. и Семенов В.А., Релейная защита энергетических систем, Москва: ЭНЕРГОАТОМИЗДАТ, 1998.
8. ГОСТ Р ИСО/МЭК 27002-2012, «Информационная технология (ИТ). Методы и средства обеспечения безопасности. Свод норм и правил менеджмента информационной безопасности».
9. Федеральный Закон № 149, «Об информации, информационных технологиях и о защите информации (с изменениями на 18 марта 2019 года)».
10. ГОСТ 27.002-89. Надежность в технике. Основные понятия. Термины и определения.
11. ISO/IEC 27002:2013 Information technology — Security techniques — Code of practice for information security controls.
12. Р 50.1.056-2005, «Рекомендации по стандартизации. Техническая защита информации. Основные термины и определения.».

13. «Доктрина энергетической безопасности Российской Федерации (утверждена Указом Президента Российской Федерации от 13 мая 2019 г. № 216)».

14. «Цифровая трансформация электроэнергетики России» в материалы конференции, http://digitenergy.ru/archive/energetics/transformation/, 2017.

15. «ЭНЕРГЕТИКИ СФОРМИРОВАЛИ ОБРАЗ ЦИФРОВОЙ ЭЛЕКТРОЭНЕРГЕТИКИ» , 05 10 2017. [В Интернете]. Available: https://minenergo.gov.ru/node/9464. [Дата обращения: 02.09.2019].

16. Министерство Энергетики Российской Федерации, «Цифровая трансформация электроэнергетики России» в «Цифровая электроэнергетика» как часть программы «Цифровая экономика Российской Федерации», Москва, 4 октября 2017.

17. ПАО Россети, «Концепция. Цифровая трансформация 2030», Москва, 2018.

18. П. Ливинский, доклад генерального директора компании «Россети» «Цифровая трансформация 2030», 21.12.2018.

19. А. Майоров, «Интернет Энергии для потребителей», корпоративная газета «Российские сети», т. 57, № 2, p. 3, 2019.

20. В.С. Кириленков и С.Ю. Вергазов, «Технические решения по РЗА, предлагаемые ПАО «Россети» в рамках создания «Цифровых подстанций»», 2018.

21. Д.В. Холкин и В.Н. Княгинин, «Цифровой переход в электроэнергетике России», Энерджинет, Москва, 2017.

22. НТИ EnergyNet, Концепция проекта «Цифровой РЭС».

23. «Особенности проектирования системы РЗА при новом строительстве и реконструкции ЦПС», НПП «ЭКРА», 2019.

24. Интегрированный годовой отчет ПАО «Федеральная сетевая компания Единой энергетической системы», 2018.

25. Д н. д. г. э. п. М. Р. Кулапин Алексей Иванович, ведомственный проект Минэнерго России «Цифровая энергетика», Москва, 01.10.2018.

26. Департамент коммуникаций Госкорпорации «Росатом», «Под эгидой Минэнерго создается центр компетенций цифровой трансформации электроэнергетики» 01 03 2019. [В интернете]. Available: https://rosatom.ru/journalist/news/pod-egidoy-minenergo-sozdayetsya-tsentr-kompetentsiy-tsifrovoy-transformatsii-elektroenergetiki/. [Дата обращения: 29 08 2019].

27. Р. В. Неуступкин, II-я Международная конференция «Цифровая подстанция. Стандарт IEC 61850», в АО «РАСУ» - интегратор в контуре ГК «Росатом» по направлениям «АСУ ТП», «Электротехника» и «Цифровая энергетика», Москва, 2-4 июля 2019 г.

28. «Интервью Председателя Правления-Генерального директора ПАО «РусГидро» Н.Г. Шульгинова в книгу «Восточный приоритет» к Восточному экономическому форуму,» 2016.

29. Карантаев В.Г. и Карпенко В.И., «Частные вопросы реализации киберзащищенной цифровой подстанции», Релейщик, № 2, pp. 39-42, 2019.

30. Z. Żurakowski, Functional Safety in Electric Power Industry Sector, Institute of Power Systems Automation, Poland, 2003.

31. Осак А.Б., Панасецкий Д.А. и Бузина Е.Я., «Кибербезопасность объектов электроэнергетики. Угрозы и возможные последствия», доклад конференции «Релейная защита и автоматика энергосистем 2014», 27-29 мая 2014.

32. Д. Даренский, «Моделирование угроз кибербезопасности в разрезе функциональной безопасности объектов электроэнергетики», доклад конференции «Релейная защита и автоматика энергосистем 2017», 25-28 апреля 2017.

33. Зегжда Д.П., Васильев Ю.С., Полтавцева М.А., Кефели И.Ф. и Боровков А.И., «Кибербезопасность прогрессивных производственных технологий в эпоху цифровой трансформации» Вопросы кибербезопасности , № 2(26, 2018 .

34. Congressional Research Service, Electric Grid Cybersecurity, 2018.

35. Е.В. Брежнев Под редакцией В.С. Харченко, «Основы анализа и обеспечения безопасности смарт грид» Tempus, 2017.

36. Массель Л.В., Воропай Н.И., Сендеров С.М. и Массель А.Г., «Киберопасность как одна из стратегических угроз энергетической безопасности России», Вопросы кибербезопасности, № 4(17), 2016.

37. Mission Support Center, National & Homeland Security Directorate и Idaho National Laboratory, Consequence-Driven, Cyber-Informed Engineering (CCE), 2016.

38. Mission Support Center и Idaho National Laboratory, Cyber Threat and Vulnerability Analysis of the U.S. Electric Sector, 2016.

39. Jason E. Stamp, Randall A. Laviolette, Laurence R. Phillips и Bryan T. Richardson, Impacts Analysis for Cyber Attack on Electric Power Systems, Sandia National Laboratories, 2009

40. Emerging Risk Report, Business Blackout. The insurance implications of a cyber attack on the US power grid, Lloyd's and the University of Cambridge Centre for Risk Studies, 2015.

41. А.К. Моторин и В.А. Харламов, «Варианты возможных векторов воздействия на оборудование РЗА в реальных условиях эксплуатации» доклад конференции «Релейная защита и автоматика энергосистем 2017», 25-28 апреля 2017.

42. НПП Экра, «Технические требования по реализации МЭК 61850 в комплексе РЗА ЦПС» доклад на НТС ЕЭС 15.08.2019, Москва, 2019.

43. ПАО «ФСК ЕЭС» и СТО 56947007-25.040.40.236-2016, «Правила технической эксплуатации АСУ ТП ПС ЕНЭС. Общие технические требования».

44. Ф. России, «Методика определения угроз безопасности информации в информационных системах» 2015.

45. IEC TS 62351-1:2007, Power systems management and associated information exchange - Data and communications security - Part 1: Communication network and system security - Introduction to security issues.

46. Ф. РФ, Приказ №236 «Об утверждении формы направления сведений о результатах присвоения объекту критической информационной инфраструктуры одной из категорий значимости либо об отсутствии необходимости присвоения ему одной из таких категорий (в ред. Приказа ФСТЭК)» 22 декабря 2017 г..

47. Otis Alexander, ICS ATT&CK, MITRE, Dec 2017.

48. Eric M. Hutchins, Michael J. Cloppert, Rohan M. Amin и Ph.D., Intelligence-Driven Computer Network Defense Informed by Analysis of Adversary Campaigns and Intrusion Kill Chains, Lockheed Martin Corporation, 2011.

49. Kaspersky Lab ICS CERT, «Ландшафт угроз для систем промышленной автоматизации» Первое полугодие 2017.

АНО ВО «Университет Иннополис»
420500, г. Иннополис, ул. Университетская, д.1
university@innopolis.ru; university.innopolis.ru
ОКПО 26762138; ОГРН 1121600006142;
ИНН/КПП 1655258235/161501001
+7 (843) 203-92-53

РЕЦЕНЗИЯ

на аналитический отчет «Анализ возможных нарушений работоспособности в результате деструктивных воздействий компьютерных атак на цифровые системы управления и защиты объектов электроэнергетического комплекса», подготовленный сотрудниками лаборатории кибербезопасности АСУ ТП компании «Ростелеком-Солар»

Актуальность работы.
В настоящее время в Российской Федерации широкое распространение получает так называемая технология интеллектуальных или «умных» энергосистем — Smart Grid. Упомянутая технология основана на использовании современных цифровых решений и предназначена для управления процессом передачи и распределения электроэнергии конечному потребителю. Реализация этой концепции предполагает повышение надежности электроснабжения потребителей, сокращение издержек и повышение прозрачности процесса управления.

Существенно, что в технологии Smart Grid ключевым является придание перспективным энергосистемам двух новых свойств.

- Сопротивление негативным воздействиям: наличие специальных методов обеспечения киберустойчивости и живучести, снижающих физическую и информационную уязвимость всех составляющих энергосистемы и способствующих как предотвращению, так и быстрому восстановлению ее после аварий в соответствии с требованиями энергетической безопасности.

- Самовосстановление при аварийных ситуациях: энергосистема и ее элементы должны быть способны постоянно поддерживать свое техническое состояние в работоспособном состоянии путем идентификации, анализа и перехода от управления по факту возникновения ситуации к превентивному (предупреждающему) управлению. Самовосстанавливающаяся энергосистема должна позволять максимально возможно минимизировать сбои (возмущения) с помощью интеллектуальной системы управления, в том числе важнейшей ее составляющей — подсистемы обеспечения кибербезопасности.

Другими словами, интеллектуальная энергосистема на основе Smart Grid должна быть проактивной по отношению к изменяющимся условиям функционирования и отслеживать надвигающиеся технические проблемы еще до того, как они смогут катастрофически повлиять на ее безопасность и устойчивость функционирования в целом. Поэтому в состав проектируемых интеллектуальных подсистем кибербезопасности должны входить соответствующие компоненты сдерживания, предупреждения, обнаружения и нейтрализации кибератак, а также самовосстановления.

Практическая значимость работы.
Представленный на рецензию аналитический отчет «Анализ возможных нарушений работоспособности в результате деструктивных воздействий компьютерных атак на цифровые системы управления и защиты объектов электроэнергетического комплекса» предназначен для выработки моделей угроз безопасности и модели нарушителей некоторых типовых объектов интеллектуальных энергосистем

(Smart Grid), а также для определения необходимых и достаточных условий для обеспечения киберустойчивости (Cyber Security) упомянутых объектов в условиях наблюдаемого беспрецедентного роста угроз безопасности.

По мере возрастания сложности современных интеллектуальных энергосистем (Smart Grid), у них возникают новые все более эмерджентные (англ. Emergent) системные свойства: киберустойчивость, управляемость, самоорганизация, проактивная кибербезопасность и адаптивность. Здесь каждое из перечисленных свойств является предметом исследования кибернетики (от греческого κυβερνητκο'ζ — искусство управления) и каждое последующее свойство имеет смысл лишь при наличии предыдущего.

Киберустойчивость (англ. Cyber Resilience) является важнейшим свойством любой интеллектуальной энергосистемы (Smart Grid), особенно в условиях перехода на шестой технологический уклад и сопутствующие технологии Индустрии 4.0: Artificial Intelligence (AI), Cloud and foggy computing, 5G+, IoT/IIoT, Big Data и ETL, Q-computing, Blockchain, VR/AR и пр. Можно даже считать его первичным, так как без него упомянутые системы как таковые не могут существовать. Действительно, без наличия устойчивого образования из связанных между собой компонентов критически важной информационной инфраструктуры не имеет смысла говорить о существовании киберсистем Индустрии 4.0. И если обеспечение кибербезопасности названных систем в основном ориентировано на оценку вероятности возникновения инцидентов и предотвращение возможных угроз безопасности, то обеспечение киберберустойчивости в большей степени направлено на сохранение целевого поведения и работоспособности интеллектуальных энергосистем (Smart Grid) в условиях как известных (примерно 45%), так и ранее не известных кибератак (оставшиеся 55%).

В настоящем отчете представлен ценный экспертный опыт и практические результаты поисковых исследований ведущих сотрудников Лаборатории кибербезопасности АСУ ТП компании «Ростелеком-Солар» по проблеме обеспечения

киберустойчивойсти (Cyber Resilience) перспективных первых отечественных интеллектуальных энергосистем (Smart Grid).

Отчет является первой известной рецензенту работой по упомянутой проблеме. При этом содержит результаты как качественного, так и начального количественного изучения киберустойчивости интеллектуальных энергосистем, что в перспективе позволит вывести предельный закон эффективности обеспечения киберустойчивости названных систем. По этой причине полученные результаты представляют несомненный практический и методический интерес для специалистов в области кибербезопасности интеллектуальных энергосистем (Smart Grid).

В отчете представлены следующие основные результаты:

- Описание типовой цифровой подстанции как объекта защиты критически важной информационной инфраструктуры электроэнергетического комплекса (согласно ФЗ-187);
- Возможные сценарии кибератак злоумышленников и оценки последствий вероятных аварий объекта ЭЭ, критически влияющих на его работу и/или работу энергосистемы в целом;
- Типовые модель угроз и нарушителя для цифровой подстанции;
- Возможная классификация кибератак на ЦПС и системы, а также наиболее вероятные сценарии проведения указанных кибератак;
- Возможные последствия кибератак на цифровую подстанцию с физическими последствиями и др.

Представленный на рецензию отчет имеет ярко выраженную практическую направленность и значимость. Полученные результаты могут быть использованы специалистами в области кибербезопасности АСУ ТП для разработки конкретных моделей угроз безопасности и нарушителей интеллектуальных энергосистем Smart Grid.

Выводы.

Принимая во внимание вышеизложенное, считаю возможным сделать следующее заключение: содержание и структура представленного на рецензирование отчета «Анализ возможных нарушений работоспособности в результате деструктивных воздействий компьютерных атак на цифровые системы управления и защиты объектов электроэнергетического комплекса», подготовленный сотрудниками Лаборатории кибербезопасности АСУ ТП компании «Ростелеком-Солар», соответствует требованиям следующих нормативных документов:

- «Доктрине информационной безопасности России», 2016 г.;
- ФЗ-187 «О безопасности критической информационной инфраструктуры»;
- «Основным направлениям государственной политики в области обеспечения безопасности АСУ ТП КВО РФ» Совета Безопасности РФ;
- Приказу ФСТЭК России от 14 марта 2014 г. №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»;
- Документам ФСТЭК по защите АСУ ТП:
  - Меры защиты в АСУ ТП;
  - Методика определения угроз безопасности информации в АСУ ТП;
  - Порядок выявления и устранения уязвимостей в АСУ ТП;
  - Порядок реагирования на инциденты, связанные с нарушением безопасности информации);
- ГОСТам Федерального агентства по техническому регулированию и метрологии – Сети коммуникационные промышленные. Защищенность (кибербезопасность) сети и системы (2016 г.):

- ГОСТ Р 56205-2014 IEC/TS 62443-1-1-200. Часть 1-1. Терминология, концептуальные положения и модели,
- ГОСТ Р МЭК 62443-2-1-2015. Часть 2-1. Составление программы обеспечения защищенности (кибербезопасности) системы управления и промышленной автоматики,
- ГОСТ Р 56498-2015/IEC/PAS 62443-3: 2008. Часть 3. Защищенность (кибербезопасность) промышленного процесса измерения и управления и др.

Представленные на рецензию материалы исследования содержат элементы новизны и оригинальности. Как следствие, считаю целесообразным рекомендовать их к практическому применению на отечественных объектах интеллектуальных энергосистем Smart Grid.

Рецензент

д.т.н., профессор _____/ Петренко С.А.
подпись

Руководитель Центра ИБ АНО ВО «Университет Иннополис»

Петренко Сергей Анатольевич

11.10.2019 г.

Подпись профессора Петренко С.А. заверяю

Руководитель отдела по работе с персоналом _____/ Ахунова Э. Р.
подпись

Ахунова Эльвира Рубисовна

+7 843 203-92-53 (120)

e.akhunova@innopolis.ru

Термины и определения

В этом разделе приведены термины, используемые в настоящем исследовании. Часть терминов взята из нормативной документации (для каждого такого термина указан первоисточник), а часть введена в этой работе.

Авария.
Технологические нарушения на объекте электроэнергетики и (или) энергопринимающей установке, приведшие к разрушению или повреждению зданий, сооружений и (или) технических устройств (оборудования) объекта электроэнергетики и (или) энергопринимающей установки, неконтролируемому взрыву, пожару и (или) выбросу опасных веществ, отклонению от установленного технологического режима работы объектов электроэнергетики и (или) энергопринимающих установок, нарушению в работе релейной защиты и автоматики, автоматизированных систем оперативно-диспетчерского управления в электроэнергетике или оперативно-технологического управления либо обеспечивающих их функционирование систем связи, полному или частичному ограничению режима потребления электрической энергии (мощности), возникновению или угрозе возникновения аварийного электроэнергетического режима работы энергосистемы [1].

Автоматизированная система технологического управления.
Единый распределенный комплекс согласованно функционирующих взаимосвязанных систем: оперативно-технологического и ситуационного управления, производственно-технического управления, мониторинга и диагностики состояния оборудования, мониторинга и управления качеством электроэнергии, РЗА, учета электроэнергии (мощности), управления электропотреблением [2].

Автоматизированное управление.
Управление, осуществляемое при совместном участии человека и средств автоматизации [2].

Автоматическое управление.
Управление, осуществляемое без участия человека [2].

Автоматизированная система управления.
Комплекс программных и программно-аппаратных средств, предназначенных для контроля за технологическим и (или) производственным оборудованием (исполнительными устройствами) и производимыми ими процессами, а также для управления такими оборудованием и процессами [3].

Автоматизированная система управления технологическими процессами.
Система, состоящая из персонала и комплекса средств автоматизации его деятельности, реализующая информационную технологию выполнения установленных функций в области управления технологическими процессами [4].

Аутентичность (authenticity).
Свойство, гарантирующее, что субъект или ресурс идентичны заявленным [5].

Безопасность информации (данных).
Состояние защищенности информации (данных), при котором обеспечены ее (их) конфиденциальность, доступность и целостность [6].

Быстродействие.
Это свойство релейной защиты, характеризующее скорость выявления и отделения от сети поврежденных элементов. Быстродействие показывает, насколько быстро средства релейной защиты реагируют на возникновение тех или иных видов повреждений [7].

Вторичное оборудование.
Оборудование (аппаратура, устройства, комплексы) АСТУ, противопожарной системы, охранной сигнализации, видеонаблюдения, СОПТ, системы собственных нужд

переменного тока 0,4 кВ, системы управления и сигнализации вспомогательного оборудования и т.п. [2].

Доступность (информации).
Состояние информации, при котором субъекты, имеющие право доступа, могут реализовывать его беспрепятственно [6].

Интеллектуальное электронное устройство.
Устройство, содержащее процессор(ы), способное получать или передавать данные, или управляющие воздействия от внешнего источника или на внешний источник, выполняющее работу заданных логических узлов в конкретном контексте и разграниченное своими интерфейсами [4].

Информационная безопасность (information security).
Защита конфиденциальности, целостности и доступности информации; кроме того, сюда могут быть отнесены и другие свойства, например, аутентичность, подотчетность, неотказуемость и надежность [8].

Информационная система.
Совокупность содержащейся в базах данных информации и обеспечивающих ее обработку информационных технологий и технических средств [9].

Источник угрозы безопасности информации.
Субъект (физическое лицо, материальный объект или физическое явление), являющийся непосредственной причиной возникновения угрозы безопасности информации [6].

Конфиденциальность (информации).
Обязательное для выполнения лицом, получившим доступ к определенной информации, требование не передавать такую информацию третьим лицам без согласия ее обладателя [9].

Коммутационный аппарат.
Электрический аппарат, предназначенный для коммутации электрической цепи и проведения тока: выключатель, разъединитель, в том числе заземляющий разъединитель [2].

Компьютерная атака.
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 информации [3].

Надежность (reliability) (технического средства).
Свойство объекта сохранять во времени в установленных пределах значения всех параметров, характеризующих способность выполнять требуемые функции в заданных режимах и условиях применения, технического обслуживания, хранения и транспортирования [10].

Надежность (информации).
Соответствие преднамеренному поведению и результатам [11].

Нарушитель безопасности информации.
Физическое лицо, случайно или преднамеренно совершающее действия, следствием которых является нарушение безопасности информации при ее обработке техническими средствами в информационных системах [12].

Неотказуемость (non repudiation).
Способность удостоверять имевшее место действие или событие так, чтобы эти события или действия не могли быть позже отвергнуты [5].

Первичное оборудование ПС.
Силовые авто(трансформаторы), системы (секции) шин, выключатели, разъединители, СКРМ, измерительные трансформаторы, преобразовательные установки и другое оборудование объектов электроэнергетики, не относящееся ко вторичному оборудованию [2].

Подотчетность (accountability).
Свойство, обеспечивающее однозначное прослеживание действий любого логического объекта [5].

Селективность.
Это свойство релейной защиты, характеризующее ее способность выявлять и отделять от электрической сети только поврежденные элементы. Другими словами, селективность — это избирательность действия [7].

Угроза безопасности информации.
Совокупность условий и факторов, создающих потенциальную или реально существующую опасность нарушения безопасности информации [6].

Угроза энергетической безопасности.
Совокупность условий и факторов, создающих возможность нанесения ущерба энергетике Российской Федерации [13].

Управляемые элементы ПС.
Коммутационные аппараты, задающие устройства систем автоматического регулирования (возбуждения синхронных электрических машин, реакторов, преобразовательных установок и др.), устройства РПН трансформаторов и автотрансформаторов, технологическое оборудование (насосы, задвижки и др.) [2].

Целостность (информации).
Состояние информации, при котором отсутствует любое ее изменение либо изменение осуществляется только преднамеренно субъектами, имеющими на него право [6].

Цифровая подстанция.
Автоматизированная подстанция, оснащенная взаимодействующими в режиме единого времени цифровыми информационными и управляющими системами и функционирующая без присутствия постоянного дежурного персонала [4].

Центр управления сетями.
Структурное подразделение сетевой организации, осуществляющее функции технологического управления и ведения в отношении объектов (части объектов) электросетевого хозяйства, находящихся в зоне эксплуатационной ответственности данной сетевой организации, или в установленных законодательством случаях в отношении объектов электросетевого хозяйства и энергопринимающих установок, принадлежащих третьим лицам [4].

Цифровая электрическая сеть.
Организационно-техническое объединение электросетевых объектов, оснащенных цифровыми системами измерения параметров режима сети, мониторинга состояния оборудования и линий электропередачи, защиты и противоаварийной автоматики, сетевого и объектового управления, информационный обмен между которыми осуществляется по единым протоколам с обеспечением синхронизации по времени [4].

Чувствительность.
Это свойство, характеризующее способность релейной защиты выявлять повреждения в конце установленной для нее зоны действия в минимальном режиме работы энергосистемы. Другими словами, защита должна чувствовать те виды повреждений и ненормальных режимов, на которые она рассчитана, в любых состояниях работы защищаемой электрической системы [7].

Энергетическая безопасность.
Состояние защищенности экономики и населения страны от угроз национальной безопасности в сфере энергетики, при котором обеспечивается предусмотренных законодательством Российской Федерации требований к топливо- и энергоснабжению потребителей, а также выполнение экспортных контрактов и международных обязательств Российской Федерации [13].

Определения, введенные в работе

Все представленные ниже термины возникли при рассмотрении вопросов обеспечения устойчивого функционирования объектов электроэнергетического комплекса, которые имеют в своем составе компоненты, обрабатывающие (под обработкой подразумевается в том числе передача) информацию в электронном виде (т.е. информационные системы, автоматизированные системы управления и информационно-телекоммуникационные сети). Такие объекты подвержены в том числе атакам, в которых происходит нарушение безопасности информации.

Однако для рассматриваемых нами объектов электроэнергетики последствия таких атак могут проявляться не только в нарушении безопасности информации, но и, что гораздо важнее, в нарушении функционирования физического (первичного) и управляющего

им вторичного оборудования. Последствия нарушений могут выражаться как в материальном ущербе, так и в ущербе жизни и здоровью людей, экологическим последствиям, т.е. последствиям, которые свойственны физическому миру. Поэтому традиционных терминов информационной безопасности нам недостаточно и есть необходимость введения новых, центральным вопросом для которых является устойчивое функционирование объекта электроэнергетического комплекса в целом.

Под устойчивостью функционирования объекта электроэнергетики понимается его способность противостоять воздействию дестабилизирующих факторов с целью поддержания возможности исполнять свои функции. Должно обеспечиваться предотвращение или ограничение угрозы жизни и здоровья людей (штатного персонала объекта и окружающего населения), нанесения материального, экологического и другого ущерба, а также обеспечения восстановления работоспособности объекта в минимально возможные сроки. В данной работе как дестабилизирующий фактор мы рассматриваем компьютерные атаки (кибератаки).

В нашем понимании объект электроэнергетики, в состав которого входят компоненты, обрабатывающие информацию в электронном виде, является примером киберфизической системы. Поэтому для полноты описания все остальные термины даны относительно понятия киберфизической системы, определение которой также вводится в настоящем исследовании.

Киберфизическая система.
Взаимосвязанная совокупность физического (первичного) оборудования, информационных систем, автоматизированных систем управления и информационно-телекоммуникационных сетей, согласованно выполняющая определенную функцию.

Кибербезопасность (в общем).
Все аспекты, связанные с определением, достижением и поддержанием состояния защищенности киберфизической системы, при котором обеспечено ее устойчивое функционирование в условиях проведения против нее кибератак.

Кибербезопасность (как состояние).
Состояние защищенности киберфизической системы, при котором обеспечено ее устойчивое функционирование в условиях проведения против нее кибератак.

Угроза кибербезопасности (киберугроза).
Совокупность условий и факторов, создающих потенциальную или реально существующую опасность нарушения кибербезопасности киберфизической системы.

Киберзащищенный (объект).
Объект, защищенный от угроз кибербезопасности (киберугроз).

Нарушитель кибербезопасности.
Физическое лицо, случайно или преднамеренно совершающее действия, следствием которых является нарушение кибербезопасности киберфизической системы.

Кибератака.
Целенаправленное воздействие программных и (или) программно-технических средств на киберфизическую систему, в целях нарушения ее устойчивого функционирования и (или) создания для нее угроз кибербезопасности.

Киберинцидент.
Факт нарушения устойчивости функционирования киберфизической системы, в том числе произошедший в результате кибератаки.

Сокращения и обозначения:

АИИС КУЭ/ АИИС ТУЭ	автоматизированная информационно-измерительная система коммерческого/ технологического учета электропотребления
АЛАР	автоматика ликвидации асинхронного режима
АОПО	автоматика ограничения перегрузки оборудования
АОПЧ/АОСЧ	автоматика ограничения повышения/ снижения частоты
АОСН/АОПН	автоматика ограничения снижения/ повышения напряжения
АРВ	автоматика регулирования возбуждения (генераторов)
АРН	автоматика регулирования напряжения
АПНУ	автоматика предотвращения нарушения устойчивости
АРКТ	автоматика регулирования коэффициента трансформации
АСККЭ	автоматизированная система контроля качества электроэнергии
АСУ ТП	автоматизированная система управления технологическим
АТ	автотрансформатор
ГРАРМ	групповое регулирование активной и реактивной мощности
ДЗГ	дифференциальная защита генератора

ДЗЛ	дифференциальная защита линии
ДЗТ	дифференциальная защита трансформатора
ДЗШ	дифференциальная защита шин
ЗН	заземляющий нож
ЗП	защита от перегрузки
ЗПУ	зарядно-подзарядное устройство
ИЭУ	интеллектуальное электронное устройство
КСЗ	комплект ступенчатых защит
ЛЭП	линия электропередачи
ОБР	оперативная блокировка разъединителей
ПА	противоаварийная автоматика
ПАС	преобразователь аналоговых сигналов
ПДС	преобразователь дискретных сигналов
ПО	программное обеспечение
ПТК	программно-технический комплекс
РА	режимная автоматика
РАС	регистратор аварийных событий
РЗ	релейная защита
РЗА	релейная защита и автоматика

РУ	распределительное устройство
САР	система автоматического регулирования
САУ	система автоматического управления
СКРМ	система компенсации реактивной мощности
СМПО	система мониторинга первичного оборудования
СМПР	система мониторинга переходных режимов
СОПТ	система оперативного постоянного тока
ТСЗ	токовые ступенчатые защиты
УПАСК	устройство передачи аварийных сигналов и команд
УПК	устройство продольной компенсации
УРОВ	устройство резервирования отказа выключателя
УСО	устройство сопряжения с объектом
УШР	управляемый шунтирующий реактор
ФОЛ	фиксация отключения линии
ФОТ	фиксация отключения трансформатора
ФОБ	фиксация отключения блока
ЦПС	цифровая подстанция
ЦУС	центр управления сетями
ЦЭС	цифровая электрическая сеть
ЧАПВ	частотное автоматическое повторное включение
ЩСН	щит собственных нужд
ЭЭ	электроэнергетика

GOOSE	Generic Object Oriented Substation Event (протокол (сервис), описанный в IEC 61850-8-1, для передачи данных по технологии «издатель-подписчики», предназначенный для передачи широковещательных сообщений (дискретных сигналов) о событиях на подстанции) [4]
MMS	Manufacturing Message Specification (протокол, описанный в IEC 61850-8-1, для передачи данных по технологии «клиент-сервер», используемый для обмена данными, результатами измерений, диагностическими сообщениями, передачи команд управления и других целей) [4]
PTP	Precision Time Protocol (протокол точного времени, используемый для синхронизации часов по компьютерной сети с точностью синхронизации менее микросекунды, что обеспечивает удобство для измерительных систем и систем управления) [4]
SCADA	Supervisory Control and Data Acquisition (диспетчерское управление и сбор данных) [4]
SNTP	Simple Network Time Protocol (протокол синхронизации времени в компьютерной сети для систем и устройств, не требующих высокой точности) [4]
SV	Sampled Values (протокол МЭК 61850-9-2 для передачи оцифрованных мгновенных величин электрической системы, неразрывно связанный с термином шина процесса – коммуникационной шиной данных, к которой подключены устройства полевого уровня подстанции (коммутационные аппараты, измерительные трансформаторы) [4]

О компании «Ростелеком-Солар»

№1
на рынке
сервисов ИБ

600+
экспертов
по кибербезопасности

70+
компаний из топ-100
российского бизнеса
под защитой

Компетенции

«Ростелеком-Солар», компания группы ПАО «Ростелеком», — национальный провайдер сервисов и технологий для защиты информационных активов, целевого мониторинга и управления информационной безопасностью.

В основе наших технологий лежит понимание, что настоящая информационная безопасность возможна только через непрерывный мониторинг и удобное управление системами защиты. Этот принцип реализован во всех продуктах и сервисах «Ростелеком-Солар».

Лицензии «Ростелеком-Солар»:

- Министерства обороны Российской Федерации — на проведение работ, связанных с созданием средств защиты информации
- ФСБ России — на проведение работ, связанных с использованием сведений, составляющих государственную тайну
- ФСБ России — на разработку, производство и распространение шифровальных (криптографических) систем
- ФСТЭК России — на деятельность по разработке и производству средств защиты конфиденциальной информации
- ФСТЭК России — на деятельность по технической защите конфиденциальности информации
- Соглашение с ФСБ России в рамках ГосСОПКА о взаимодействии по предупреждению кибератак

Содержание

Авторы

Владислав Карпенко · Владимир Карантаев
Сергей Парьев · Андрей Кузнецов · Дмитрий Сютов
Евгений Дружинин · Илья Карпов

Контактная информация

Телефоны:

+7 (499) 755-07-70 — продажи и общие вопросы
+7 (499) 755-02-20 — техническая поддержка

E-mail:

info@rt-solar.ru
support@rt-solar.ru

Адреса:

125009, Москва, Никитский пер., 7, стр. 1
127015, Москва, ул. Вятская, 35/4, БЦ «Вятка», 1-й подъезд


Ростелеком
Солар