Москва, 29 сентября - 1 октября

МЕЖДУНАРОДНАЯ КОНФЕРЕНЦИЯ И ВЫСТАВКА

РЕЛЕЙНАЯ ЗАЩИТА И АВТОМАТИКА ЭНЕРГОСИСТЕМ 2021

Влияние человеческого фактора на кибербезопасность объектов электроэнергетики в эпоху тотальной цифровизации

А.Б. Осак, Д.А. Панасецкий, Е.Я. Бузина

ИСЭМ СО РАН

Россия

Осак Алексей Борисович

Введение

Последнее десятилетие идут активные дискуссии на тему цифровых подстанций и внедрения решений для электроэнергетики на базе протокола МЭК 61850, эти дискуссии проходят на фоне процесса внедрения этих технологий на энергообъекты.

Последние годы начата активная дискуссия и практические шаги в направлении тотальной цифровизации и цифровой трансформации электроэнергетики.

Большую важность имеет обеспечение кибербезопасности систем автоматического управления, таких как устройства релейной защиты (РЗ), устройства режимной и противоаварийной автоматики (РА и ПА), системы АСУ ТП.

Введение

Введение

В будущем, в эпоху тотальной цифровизации, кибератаки или иные негативные способы воздействия на цифровую инфраструктуру критически важных инфраструктурных объектов и систем, к которым относится ЕЭС, станут элементами геополитического и военного противостояния, о чем уже сегодня публично говорят высокопоставленные лица различных государств мира.

Следует ожидать как кибератак со стороны профессиональных хакеров, квалификация которых существенно выше квалификации большинства специалистов энергопредприятий, так и подкупа специалистов энергопредприятий (или иной формы принуждения их работать на потенциального противника).

Введение

Введение

Эти типичные проблемы любой защиты и обороны, т.к. нападающая сторона может сконцентрировать все усилия на одном участке, привлечь лучших специалистов, выделить на атаку большие финансовые средства.

Не зная место и время нападения, защиту и оборону придется обеспечивать по всем объектам и системам, что вызывает распыление сил и средств, и как следствие, закономерный недостаток этих сил и средств, в т.ч. кадровых в месте полномасштабной атаки.

Если враждебные воздействия на цифровую составляющую критически важных инфраструктурных объектов и систем станут элементами геополитического и военного противостояния, то в месте полномасштабной комплексной атаки, гарантированно будут преодолены все эшелоны киберзащиты.

Цифровые системы управления

Известно, что функционирование ЭЭС возможно только при соответствующем непрерывном управлении, как отдельными электроустановками, так и ЭЭС в целом.

Эффективное и адекватное оперативно-диспетчерское и противоаварийное управление является одним из факторов определяющим надежность ЭЭС.

Цифровые технологии, микропроцессорная техника со значительными вычислительными ресурсами позволяют создавать достаточно сложные и совершенные алгоритмы управления ЭЭС для оперативно-диспетчерского управления нормальными режимами и противоаварийного управления.

Угрозы

Как бы ни совершенствовались в устойчивости к кибератакам программные и аппаратные средства, выполняющие прикладные и коммуникационные функции на энергообъектах, и какие бы дополнительные специальные технические средства ни применялись для защиты от кибератак, все это не решает проблему человеческого фактора.

Проблемы человеческого фактора наиболее остро будут стоять при автоматизации распределительных электрических сетей, на объектах малой распределенной генерации, при интеграции активных потребителей в общий контур управления режимом ЭЭС.

Угрозы

Понятие термина безопасность (в т.ч. кибербезопасность) не ограничивается состоянием защищенности только от внешних угроз. Не менее важным аспектом является обеспечение защищенности от внутренних угроз, к которым в том числе относятся недостатки и ошибки в программном обеспечении.

Киберугрозы – это выполнение непредусмотренных функций от несанкционированной передачи информации третьим лицам, до реализации зловредных функций, что можно трактовать как частичный или полный отказ системы управления энергообъектом.

Угрозы

Возможные угрозы (возмущающих факторов) с позиции кибербезопасности для современных электроэнергетических объектов :

- внутренние угрозы:
  - Невыявленные ошибки в программном обеспечении устройств электроэнергетического объекта;
  - Ошибки оперативного и эксплуатационного персонала энергообъекта.
- внешние угрозы:
  - Злонамеренные программные дефекты (закладки), встроенные в программное обеспечение микропроцессорных устройств электроэнергетического объекта, с целью управляемого вывода из строя системы;
  - Кибератаки извне, через внешние цифровые каналы связи энергообъекта;

Качественная оценка надежности современных систем РЗ, ПА и РА

Оценка надежности любой системы связана с оценкой вероятности и масштабов последствий отказов элементов системы.

Можно выделить следующие виды отказов для систем автоматического управления в электроэнергетике (РЗ, ПА и РА):

- **Отказы аппаратной части микропроцессорной вычислительной системы;**
- **Отказы органов сопряжения и ввода-вывода;**
- **Ошибки в прикладных алгоритмах;**
- **Ошибки в программном обеспечении;**
- **Ошибки в настройках.**

Испытания цифровых устройств

Важно понимать, что программное обеспечение современных контроллеров и терминалов содержит сотни тысяч или даже миллионы строк программного кода и команд машинного кода.

Рассматривая готовое изделие как «черный ящик», путем проведения внешних испытаний даже теоретически невозможно обнаружить все возможные ошибки.

На практике, требуется проведение очень ограниченного числа испытательных опытов, которое исчисляется десятками или сотнями, что на несколько порядков меньше, чем число строк программного кода.

Чтобы получить надежно работающий аппаратно-программный продукт недостаточно внешних испытаний методом «черного ящика».

Качество программного обеспечения

Для разработки корректно работающего (безошибочного) программного обеспечения необходимо использовать целый комплекс организационных, методических и технических средств, начиная с подбора кадров и повышения их квалификации.

Тестирование необходимо выполнять, начиная с автоматической или автоматизированной проверки работоспособности каждой программной процедуры, даже содержащей всего несколько строк программного кода.

Но все это существенно увеличивает первоначальную стоимость программного продукта. И на уровне конкурсных процедур при закупке оборудования, где ценовой критерий решающий, избыточная себестоимость не будет способствовать выбору в пользу качественного программного продукта.

Аспекты кибербезопасности

Первый аспект, без учета потенциальных массированных кибератак со стороны геополитических противников;

Второй аспект в части минимизации потенциального ущерба от кибератак со стороны геополитических противников.

Опасность неправильной и ложной работы цифровых устройств

Еще одна проблема связана с фактическим наличием больших объемов управляющих воздействий у реальных устройств и комплексов РЗ и ПА.

Например, некоторые комплексы ЛАПНУ имеют управляющие воздействия на отключение нагрузки и генерации суммарным объемом в несколько ГВт.

Это все хорошо, пока работает правильно, но ложная работа таких комплексов может быть инициатором системой аварии.

Можно в целом сказать, что многие системные аварии, в т.ч. аварии в ЕЭС 22.08.2016 г. и 27.06.2017 г. переросли из локальных в общесистемные аварии по причине несовершенства алгоритмов комплексов ПА.

Системная авария в ОЭС Сибири 27.06.2017

Эта системная авария в ОЭС Сибири непосредственно связана с некорректной и незапланированной работой нескольких современных цифровых комплексов ПА, РЗ и РА.

Во время данной аварии не было ни одного короткого замыкания или повреждения первичного силового оборудования, но объем отключенной генерации составил около 7 ГВт, отключенной нагрузки около 4 ГВт.

Качественная оценка надежности современных систем РЗ, ПА и РА

Методические указания по устойчивости энергосистем в качестве нормативных возмущений рассматривают только отключение элементов ЭЭС вследствие КЗ и работы основных и резервных РЗ.

Рассматривается только отказ основных защит (несрабатывание) и отказ выключателя с работой УРОВ.

Ложная работа РЗ, РА и ПА не рассматривается в качестве нормативных возмущений.

Стандарты по противоаварийному управлению рассматривают только отказ в срабатывании, требуя дублирования устройств ПА.

Требования про недопустимость ложной работы носят декларативный характер.

Качественная оценка надежности современных систем РЗ, ПА и РА

Соответственно, предлагается рассматривать отказы систем автоматического управления разных видов при проектировании и планировании развития энергосистем.

Как минимум, нужно учитывать возможность ложной работы любого устройства в виде выдачи самого большого или самого неблагоприятного управляющего воздействия.

Любой терминал РЗ или ПА вследствие некого отказа может одновременно выдать все подключенные управляющие воздействия, даже если их сочетание не предусмотрено прикладным алгоритмом, т.к. такой отказ может быть вызван ошибкой в программном обеспечении.

Такие отказы не должны быть неожиданностью для эксплуатирующих организаций и диспетчерских центров. Эти вопросы должны прорабатываться заранее, начиная с ПИР и далее в процессе эксплуатации.

Особенности целенаправленных внешних кибератак

Когда происходят целенаправленные внешние кибератаки, инициированные иностранными государствами или крупными корпорациями, то на их реализацию могут быть выделены существенные ресурсы, как финансовые, так и кадровые.

Квалификация атакующих хакеров может быть значительно выше, чем квалификация специалистов на объектах электроэнергетики.

Если техническими средствами кибератака блокируется, то возможен подкуп, шантаж или обман специалистов на объектах электроэнергетики, или специалистов инжиниринговых компаний или предприятий производителей технических средств для электроэнергетики.

Особенности целенаправленных внешних кибератак

Особенности целенаправленных внешних кибератак

В условиях всеобъемлющего использования смартфонов, умных гаджетов, социальных сетей и прочих инструментов цифровых коммуникаций, задача подкупа, шантажа или обмана специалистов существенно упрощается, если этим занимаются представители спецслужб иностранных государств.

Для этих целей доступна достаточно полная информация о самом специалисте, составе его семьи, интересах, хобби, друзьях и прочем. Доступны контакты и сведения о близких членах семьи, включая их текущее местоположение, аудио, фото и видеоматериалы.

Важно отметить, что речь идет об обычных специалистах, а не об офицерах спецслужб, т.е. люди не давали юридически и морально обязывающей присяги на рабочем месте, не имеют специальной подготовки и т.п.

Особенности целенаправленных внешних кибератак

Особенности целенаправленных внешних кибератак

Поэтому, если не этот, так другой специалист, если не на этом, так на другом энергообъекте поддастся на подкуп, шантаж или обман, соответственно, откроет доступ, отключит средства защиты и т.д.

Поэтому вероятность успешной атаки подобного рода составляет практически 100%.

При этом подготовительная стадия будет незаметна со стороны самого объекта электроэнергетики, т.е. атака вероятнее всего будет неожиданной.

Негативные последствия целенаправленных кибератак

Одновременный отказ большого числа цифровых устройств РЗА одного производителя на одном или группе энергообъектов, находящихся в одном информационном пространстве, имеющем физическую связь с интернетом. При этом логические защиты типа межсетевых экранов или маршрутизации могут быть отключены в рамках данной атаки.

Одновременный отказ большого числа внутриобъектовых и межобъектовых цифровых сетей (каналов) связи, находящихся в одном информационном пространстве, имеющем физическую связь с интернетом или каналами связи общего доступа.

Одновременное получение доступа к большому числу цифровых устройств РЗА одного производителя, находящихся в одном информационном пространстве, что приведен к смене настроек и алгоритмов работы или к телеуправлению, в т.ч. для создания аварийной ситуации.

Негативные последствия целенаправленных кибератак

Важно отметить, что принципы ближнего и дальнего резервирования в РЗ, а также принципы эшелонированного построения ПА не предполагают одновременного и массового выхода из строя большого числа защит и автоматик.

Соответственно, возможны неустранимые КЗ, работа оборудования в режиме перегрузок и другие аварийные ситуации, которые могут привести к повреждению первичного оборудования.

Еще одним серьезным последствием кибератаки подобного рода является большое время восстановления ЭЭС после атаки.

Учитывая полную зависимость всех сфер экономики и современного социума от наличия электроснабжения, то нарушение электроснабжения большого числа потребителей одновременно с большим временем восстановления носит уже катастрофический характер.

Факторы влияющую на киберзащищенность

Универсализм цифровых решений, унификация цифровых интерфейсов, аппаратных платформ, операционных систем, наличие централизованных средств администрирования, общее информационное пространство на физическом уровне, существенно увеличивают вероятность широкомасштабных кибератак, т.к. увеличивают потенциальный ущерб от успешной кибератаки.

Разнородность решений, их несовместимость, отсутствие интеграции в единое информационное пространство, снижают вероятность широкомасштабных кибератак, т.к. ограничивается потенциальный ущерб от успешной кибератаки по причине ограниченного числа устройств и систем, которые могут быть подвергнуты атаке такого рода.

Факторы влияющую на киберзащищенность

При построении систем автоматического управления в электроэнергетики в эпоху тотальной цифровизации необходимо придерживаться эшелонированного принципа, где системы последнего эшелона должны быть либо изолированными, либо минимально интегрированными в цифровые системы управления.

Если дорогостоящая кибератака, требующая участия уникальных специалистов-хакеров не приведет к существенному ущербу, и не приведет к значимому увеличению времени восстановления ЭЭС после аварии, вызванной кибератакой, то и целесообразность такой атаки становится далеко не очевидной при геополитическом или военном противостоянии.

Факторы влияющую на киберзащищенность

Еще одним из возможных вариантов решения проблемы является установка на энергообъектах оборудования фиксированной функциональности (с жесткой логикой) для ограничения доступа и взаимодействия с внешними сетями, настройки и режимы работы которого, персонал энергообъекта не может изменить без использования специализированного оборудования.

При необходимости изменения настроек, такое оборудование отправляется на завод изготовитель (в специализированный сервисный центр), где все изменения вносятся с помощью специальных устройств.

Такой подход будет наиболее целесообразен для применения на генерирующих объектах средней мощности, а тем более в распределительных электрических сетях, на объектах малой генерации и у активных потребителей, где имеются проблемы с квалификацией персонала и текучестью кадров.

СПАСИБО ЗА ВНИМАНИЕ!

Контакты: osakalexey@mail.ru
+7-964-54-29-722
+7-914-870-59-34
Осак Алексей Борисович