Осак А.Б.[1], **Бузина Е.Я.**[2] ©
[1]Научный сотрудник; [2]старший инженер.
Институт систем энергетики им. Л.А. Мелентьева СО РАН

ВЛИЯНИЕ ЧЕЛОВЕЧЕСКОГО ФАКТОРА ПРИ ОБЕСПЕЧЕНИИ КИБЕРБЕЗОПАСНОСТИ НА НАДЕЖНОСТЬ ОБЪЕКТОВ ЭЛЕКТРОЭНЕРГЕТИКИ И ЖИВУЧЕСТЬ ЭЛЕКТРОЭНЕРГЕТИЧЕСКИХ СИСТЕМ

Аннотация

В статье показывается, что наибольшую угрозу кибербезопасности для важных инфраструктурных систем, какой является электроэнергетическая отрасль, представляет собой человеческий фактор, причем главным образом среди специалистов, которые должны обеспечивать кибербезопасность. Предлагается на энергообъектах с цифровыми и микропроцессорными системами защиты и управления выделять наиболее важные (критические) функции защит от повреждения оборудования, и реализовывать их не на цифровой базе, тем самым, исключая саму возможность кибератаки на эти критически важные подсистемы.

Ключевые слова: кибербезопасность, электроэнергетическая система, надежность, живучесть.

Keywords: cyber security, power system, reliability, survivability.

Инфраструктурная важность электроэнергетики для существования, жизнеобеспечения и развития государства и общества, а также непрерывность и нераздельность процессов производства, передачи, распределения и потребления электрической энергии приводит к повышенной значимости задач по обеспечению безопасности, надежности и живучести электроэнергетических систем (ЭЭС) и их объединений [1; 2].

В последнее время, в электроэнергетике все большее значение играют информационные и цифровые технологии, которые все шире используются для решения задач управления. Вопросы надежности компьютерных подсистем и кибербезопасности современных электроэнергетических объектов, оснащенных цифровыми устройствами релейной защиты (РЗ), противоаварийной автоматики (ПА), системами мониторинга и управления (АСУ ТП), становятся очень актуальными вследствие новизны проблемы [3; 4].

В большинстве публикаций и нормативных документах, посвященных вопросам кибербезопасности в целом [5; 6] и кибербезопасности объектов электроэнергетики в частности [4; 7], основным способом ее обеспечения видится применение соответствующих технических средств, которые обеспечивают требуемую защиту от различных несанкционированных действий [8].

Авторы, не отрицая необходимость применения специальных технических средств обеспечивающих кибербезопасность, предлагают посмотреть на данную проблему с позиции человеческого фактора [9], так как именно человек (сотрудник энергопредприятия, сотрудник поставщика и подрядчика, или стороннее лицо) является основной причиной потенциальной киберугрозы. Предлагается подход к анализу киберугроз, с классификацией возможных последствий и ущербов, с прослеживанием причинно-следственной связи по всей цепочке [10; 11].

Надежность электроэнергетической системы обеспечивается двумя категориями:

• Первая – надежность функционирования всей производственной цепочки: производство электроэнергии, ее транспорт и распределение до электроустановок

потребителей. Ключевая роль здесь отводится надежности основного электроэнергетического оборудования, которая обеспечивается соответствующими мероприятиями на этапах жизненного цикла (проектирования, производства, монтажа, наладки, эксплуатации).

• Вторая – адекватность и эффективность управления. Известно, что функционирование ЭЭС возможно только при соответствующем непрерывном управлении, как отдельными электроустановками, так и ЭЭС в целом.

Цифровые технологии, микропроцессорная техника со значительными вычислительными ресурсами позволяют создавать в рамках ЭЭС достаточно сложные и совершенные алгоритмы управления как в рамках оперативно-диспетчерского управления нормальными режимами, так и противоаварийного управления. Это в сочетании с новым поколением первичного оборудования, имеющим высокие эксплуатационные характеристики, и обладающим возможностями мониторинга и управления, позволяет повысить общую надежность ЭЭС.

С другой стороны цифровым технологиям и микропроцессорной технике свойственна возможность резкого изменения своего функционала путем перепрограммирования, которая, при правильном применении, позволяет совершенствовать технологии и алгоритмы управления без замены оборудования. Но именно это и является основой новых видов угроз для ЭЭС – угроз кибербезопасности.

Киберугрозы [12; 13] по своей сути – это выполнение непредусмотренных функций, от несанкционированной передачи информации третьим лицам, до выполнения зловредных функций, то есть по сути частичный или полный отказ системы управления энергообъектом .

В качестве возможных угроз (возмущающих факторов) с позиции кибербезопасности для современных электроэнергетических объектов можно отметить следующие [14]:

• невыявленные ошибки в программном обеспечении, вследствие чего РЗ, ПА и АСУ ТП энергообъекта работают по неверному алгоритму;

• злонамеренные программные дефекты (закладки), встроенные в программное обеспечение микропроцессорных устройств энергообъекта, с целью управляемого вывода из строя этих устройств;

• кибератаки извне, через внешние цифровые каналы связи энергообъекта, путем перехвата каналов телемеханики, телеуправления или встраивания зловредного программного кода в объектовые системы управления;

• ошибки оперативного и эксплуатационного персонала энергообъекта, которые приводят к снятию систем защиты внешних каналов связи, к замене программного обеспечения на непроектный вариант, к заражению вирусами и др.

Ключевыми элементами, которые могут быть подвержены кибератаке с последующим нарушением функционирования цифровой подстанции являются [15]:

• коммуникационные сети энергообъекта, включая коммутаторы и маршрутизаторы, в том числе шины процессов и шины объектов (в соответствии с МЭК-61850), которые в рамках концепции «цифровой подстанции» являются неотъемлемыми элементами любой функции РЗА, ПА, АСУ ТП;

• цифровые устройства РЗА, ПА, АСУ ТП;

• внешние цифровые каналы, по которым осуществляется технологическая и оперативная связь с другими энергообъектами и диспетчерскими пунктами.

С одной стороны, совершенствование технических и программных средств, выполняющих коммуникационные функции на современных энергообъектах, а также применение специальных технических и программных средств, предназначенных для защиты от кибератак, снижает вероятность атаки извне и последствия от возможных невыявленных ошибок в программном обеспечении. Но с другой стороны, ключевой проблемой кибербезопасности является то, что одно и то же устройство или программное обеспечение может быть настроено так, чтобы обеспечивать кибербезопасность и недопускать кибератаки, а может быть настроено по-другому, т.е. способствовать

кибератакам, выполнять заведомо зловредные функции в процессе кибератаки, чего нельзя было сказать об устройствах на традиционных подстанциях (особенно на электромеханической базе). Внешний вид устройств при этом не меняется, однако их функциональность в части кибербезопасности принципиально разная. Отличие исключительно в настройках, причем отличаться может незначительное число параметров из тысячи совпадающих. Дилетант в вопросах кибербезопасности вообще не сможет выявить проблему путем каких-то периодических осмотров оборудования. Поэтому, требуется привлечение специально обученных специалистов, которые способны решать подобные задачи.

Если все устройства РЗА, ПА, системы управления первичным оборудованием будут выполнены на цифровой базе и будут объединены в единую информационно-управляющую систему, то результатом кибератаки может быть полная потеря управляемости энергообъектом или заведомо ложное управление. В результате кибератаки возможна даже перепрошивка цифровых устройств или удаление на них системного и прикладного программного обеспечения, в этом случае для восстановления работоспособности потребуется полный цикл пуско-наладочных работ длительностью до нескольких месяцев. Если несколько смежных подстанций подвергнется целенаправленной кибератаке, то вполне возможны случаи полного обесточивания значительной группы потребителей (включая ответственных). Также возможны случаи повреждения дорогостоящего первичного оборудования вследствие неустраненного короткого замыкания или длительной неустраненной перегрузки. При этом классические средства дальнего резервирования на смежных цифровых подстанциях могут быть также неработоспособны по все той же причине [16].

Рассматривая угрозы кибербезопасности для оценки важности мероприятий, в том числе дорогостоящих, по повышению кибербезопасности электроэнергетических объектов, важно отметить некоторые возможные мотивы к осуществлению различных кибератак.

Первый мотив – геополитическое противостояние и военные угрозы [17; 18]. Ежегодно многие государства тратят миллиарды долларов на закупки вооружения и содержание многочисленных армий, при этом, безусловно, возникает большой соблазн нанести упреждающий удар по инфраструктуре противника (а электроэнергетика – это важнейшая инфраструктурная отрасль любой развитой экономики), не вовлекая в это собственно вооруженные силы. В 2013 году, на фоне скандальных событий с Эдвардом Сноуденом, были озвучены многочисленные факты информационного слежения посредством цифровых технологий за государственными органами власти многих стран мира со стороны специальных служб США. По существу, данные факты можно квалифицировать, как непрерывные кибернетические атаки на государственные органы власти, причем данные атаки не были выявлены органами безопасности атакованных государств, а стали известны только благодаря шпионскому скандалу.

Второй мотив – коммерческий. Крупнейшие электроэнергетические компании являются акционерными обществами (корпорациями), акции которых торгуются на биржевых площадках. Можно с уверенностью предположить, что акции компании, серьезно пострадавшей от массированной кибератаки, существенно упадут в цене, что делает их привлекательными для покупки потенциальными инвесторами. Учитывая многомиллиардную стоимость крупных электроэнергетических компаний, полученная таким образом выгода может исчисляться сотнями миллионов или даже миллиардами долларов. Всего лишь два приведенных выше примера, показывают, что потенциально возможен серьезный спрос на кибератаки объектов и систем электроэнергетики.

Вероятность целенаправленных кибератак зависит главным образом от двух составляющих:

• Цена «услуг взлома»;

• Масштаб последствий.

Чем выше негативный масштаб последствий, тем большую цену будет готов заплатить потенциальный заказчик кибератаки. При большой цене за «услуги взлома» решающую роль будет играть лояльность специалистов. Соответственно масштаб последствий, по сути, и определяет вероятность серьезной кибератаки.

Традиционные подходы к кибербезопасности электроэнергетических объектов, основаны на предположении о 100% адекватности, квалифицированности, внимательности, дисциплинированности, честности, лояльности всех сотрудников, в том числе производителей, проектировщиков, наладчиков и эксплуатационных организаций. Но, если активное сетевое оборудование и системы контроля доступа заведомо настроить неправильно, то с любой точки планеты можно будет буквально за несколько минут нарушить функционирование любого энергообъединения, даже такого масштабного, как ЕЭС России (ЕЭС/ОЭС). В традиционной энергетике, хотя бы расстояния между энергообъектами играли роль защитного барьера.

Поэтому, важнейшим требованием к специалисту по кибербезопасности является требование правильного и добросовестного выполнения своих обязанностей. Однако, учитывая масштаб последствий, а также то, что заинтересованными сторонами в кибератаке могут быть иностранные государства, на первый план выходят вопросы политической и бизнес лояльности, патриотизма, эффективности спецслужб и т.п. То есть вопросы, выходящие за рамки техники и энергетики. Если ничего не предпринимать, то можно говорить о том, что любая цифровая подстанция должна превращаться в некий закрытый и секретный объект, наподобие военных и ядерных объектов, со всеми вытекающими затратами. Но готов ли электроэнергетический бизнес к такому?

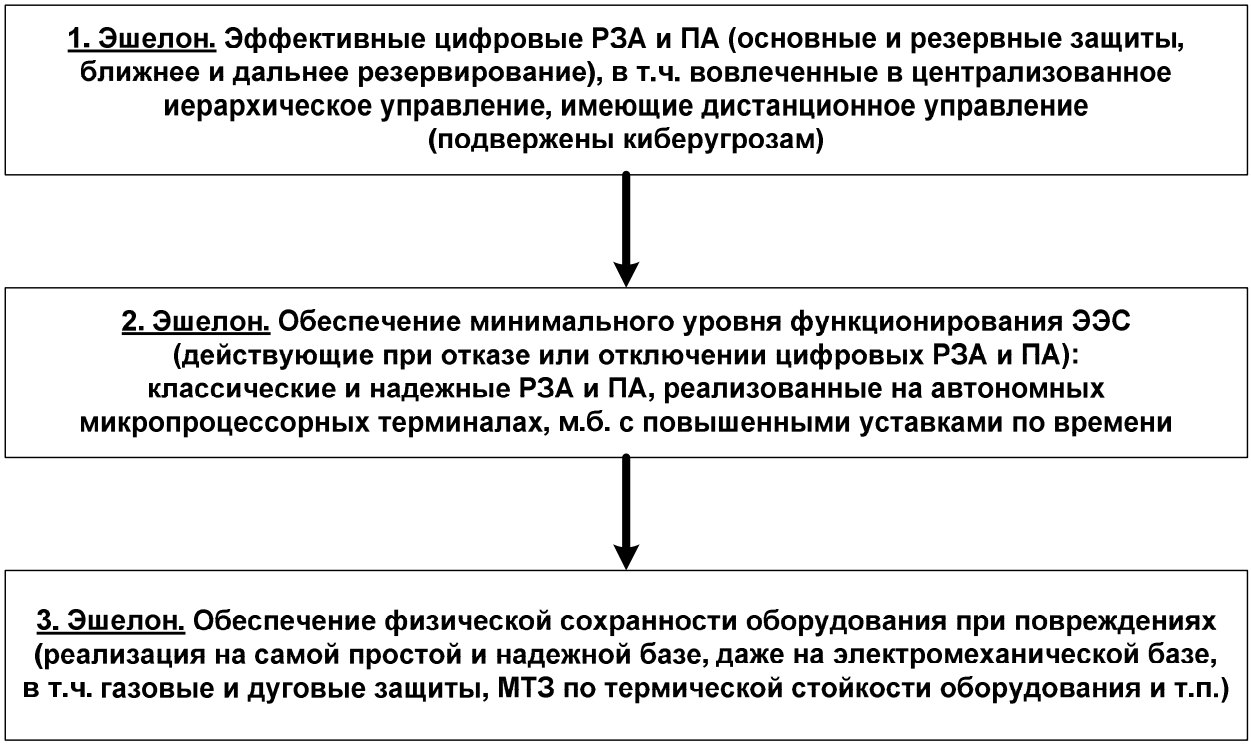

Рис. 1. **Вариант решения проблемы кибербезопасности путем совмещения цифровых, аналоговых и электромеханических устройств**

Как было отмечено выше, успешность кибератаки зависит не только от качества технических средств, но и от слабоуправляемых процессов, таких как лояльность и человеческий фактор. Поэтому одним из наиболее важных аспектов, который необходимо обеспечивать с позиции кибербезопасности энергообъектов, является то, чтобы успешная кибератака не приводила к повреждению дорогостоящего или сложно ремонтируемого оборудования. Соответственно необходимо хотя бы в минимально допустимом по условиям эксплуатации объеме сохранять в условиях кибератаки функции защиты и управления, выполненные без использования современных цифровых технологий, и не вовлеченные в сферу управления интегрированных цифровых устройств. Это позволит быстро восстановить работоспособность энергообъекта, даже если цифровые устройства полностью выведены из строя в результате кибератаки (требуют полного объема пуско-наладочных работ). Поэтому некоторое совмещение цифровых, аналоговых и электромеханических устройств может являться простым и эффективным средством обеспечения кибербезопасности, так как существенно снижается масштаб последствий от кибератаки, причем данное решение будет полностью понятным электроэнергетикам (см. рис.1).

На организационном уровне необходимо принципиально переработать подходы к лицензированию специалистов. Учитывая общую сложность цифровых технологий и применяемых алгоритмов цифровой коммуникации, необходимо обратить внимание на персональное лицензирование конкретных специалистов. Сейчас допуск на определенные виды работ выдается организации в целом, а необходимо этот допуск давать конкретным специалистам, без привязки к организации, тогда существенно повышается персональная ответственность специалиста, и снижается возможность административного давления. Следует отметить, что подобный способ лицензирования специалистов успешно применяется в США.

Литература

1. Бушуев В.В., Каменев А.М., Кобец Б.Б. Энергетика как инфраструктурная «система систем» // Общественно-деловой журнал «Энергетическая политика» №5, 2012. с. 3-15.
2. Воропай Н.И., Осак А.Б. Электроэнергетические системы будущего. // Общественно-деловой журнал «Энергетическая политика» №5, 2014. с.60-63.
3. Hong J., Liu C.-C., Govindarasu M. Integrated anomaly detection for cybersecurity of the substations. // IEEE Transactions on Smart Grid, vol. 5, №4, July, 2014, pp. 1643–1653,.
4. Нудельман Г.С. О требованиях кибербезопасности систем РЗА при использовании МЭК 61850. // Сборник докладов XXI конференции «Релейная защита и автоматика энергосистем», Москва, 29-31 мая 2012, с. 18-23.
5. Требования 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, утверждены приказом № 31 ФСТЭК России от 14.03. 2014 г.
6. Згоба А.И., Маркелов Д.В., Смирнов П.И. Кибербезопасность: угрозы, вызовы, решения. // Журнал «Вопросы кибербезопасности», №5(8), 2014. с.30-38.
7. Никандров М.В., Брагута М.В. Концепция построения комплекса кибербезопасности информационной инфраструктуры современных объектов электросетевого хозяйства. // Сборник докладов международной конференции «Современные направления развития систем релейной защиты и автоматики энергосистем», Сочи, 1 – 5 июня 2015 г.
8. Калашников А.О. Управление информационными рисками объектов критической информационной инфраструктуры Российской Федерации. // Журнал «Вопросы кибербезопасности», №3(4), 2014. с.35-41.
9. Осак А.Б., Панасецкий Д.А., Бузина Е.Я. Человеческий фактор при обеспечении кибербезопасности объектов электроэнергетики. // Сборник докладов международной конференции «Современные направления развития систем релейной защиты и автоматики энергосистем», Сочи, 1 – 5 июня 2015 г.

10. Осак А.Б., Панасецкий Д.А., Бузина Е.Я. Кибербезопасность объектов электроэнергетики. Угрозы и возможные последствия. // Сборник докладов XXII конференции «Релейная защита и автоматика энергосистем», Москва, 27-29 мая 2014, с. 417-423.
11. Гордейчик С.В. Миссиоцентрический подход к кибербезопасности АСУ ТП. // Журнал «Вопросы кибербезопасности», №2(10), 2015. с.56-59.
12. Безкоровайный М.М., Татузов А.Л. Кибербезопасность – подходы к определению понятия. // Журнал «Вопросы кибербезопасности», №1(2), 2014. с.22-27.
13. Алпеев А.С. Терминология безопасности: кибербезопасность, информационная безопасность. // Журнал «Вопросы кибербезопасности», №5(8), 2014. с.39-42.
14. Духвалов А.П. Кибератаки на критически важные объекты – вероятная причина катастроф. // Журнал «Вопросы кибербезопасности», №3(4), 2014. с.50-53.
15. Осак А.Б, Панасецкий Д.А., Бузина Е.Я. Аспекты надежности и безопасности при проектировании цифровых подстанций // Сборник докладов международной конференции «Современные направления развития систем релейной защиты и автоматики энергосистем», Екатеринбург, 3 – 7 июня 2013 г.
16. Гуревич В.И. Уязвимость современной релейной защиты: поможет ли защита от кибератак? // Журнал «ЭнергоРынок», №9, 2013. с.40-44.
17. Бородакий Ю.В., Добродеев А.Ю., Бутусов И.В. Кибербезопасность как основной фактор национальной и международной безопасности XXI века (часть 1). // Журнал «Вопросы кибербезопасности», №1, 2013. с.2-9.
18. Бородакий Ю.В., Добродеев А.Ю., Бутусов И.В. Кибербезопасность как основной фактор национальной и международной безопасности XXI века (часть 2). // Журнал «Вопросы кибербезопасности», №1(2), 2014. с.5-12.