Антон Моторин

Я считаю, что в настоящее время угроза кибербезопасности становится все более актуальной.

ТЭК России находится в состоянии постоянной (зачастую стохастической и бессистемной) модернизации, особенно в части систем релейной защиты и автоматики. Как следствие этого процесса, возникает множество частично реконструируемых объектов с различными уровнями цифровизации вторичных систем и разными уровнями доступа как к устройствам РЗА, ПА, так и к системам передачи сигналов РЗА и ПА (например, система FOXMAN для управления модулями TEBIT в FOX515 и TEPI в FOX615).

В результате появляются в первую очередь косвенные проблемы, связанные с кибербезопасностью, которые не приводят к моментальному появлению неисправностей, а носят скорее накопительный характер и становятся «бомбой замедленного действия»:

- низкоквалифицированный обслуживающий персонал (ошибки при самостоятельном параметрировании терминалов и т.д.);
- несоблюдение правил доступа к оборудованию (применение одинаковых паролей, возможность несанкционированного доступа к журналу паролей и т.д.);
- возможность попадания на АРМ различного вредоносного ПО (особенно стоит обратить внимание на переносное АРМ, с которого осуществляется наладка МП-терминалов РЗА).

Но, кроме косвенных угроз, можно выделить и прямые:

- возможность доступа к индивидуальным MUX через централизованные системы управления и контроля оборудования ЦСПИ (дистанционный доступ к MUX, снабженным модулями приема/передачи команд РЗА);

- возможность удаленного доступа через ЦУС к системе автоматизации подстанции по протоколу TCP/IP.

Также следует учитывать и постепенное распространение цифровых технологий на объектах энергетики (концепция ЦПС, Smart Grid и т.д.), что может расширить перечень возможных направлений несанкционированного доступа.

Очень важным моментом в вопросах кибербезопасности является создание моделей угроз и моделей нарушителей, потому что только аналитика по этим направлениям позволит определить уязвимости и пути их контроля с учетом внешних и внутренних факторов воздействия.

> Реализация программных и аппаратных средств защиты будет особенно необходима при массовой цифровизации объектов энергетики (концепция ЦПС, Smart Grid и т.д.).

Следует также отметить некое противопоставление системы кибербезопасности и возможности физического воздействия на объекты электроэнергетики (наброс закороток, различные виды физического повреждения оборудования и т.д.), которое имеет место при обсуждении самой концепции кибербезопасности. Я считаю, что сравнивать эти понятия не имеет смысла, так как мы должны в первую очередь говорить о конструктивном подходе, который позволит решить проблему до ее полномасштабного развития, а не рассматривать противопоставляемые понятия, обсуждение которых в данном ключе ни к чему не приводит. Ярким примером отставания и перехода к неконструктивному диспуту является обсуждение темы ЦПС и МЭК 61850, которое длится уже с десяток лет и ни к чему не приводит. Несмотря на это продолжается внедрение принятых технических решений при отсутствии соответствующей нормативной базы как для проектирования, так и для эксплуатации.

Я считаю, что реализация программных и аппаратных средств защиты будет особенно необходима при массовой цифровизации объектов энергетики (концепция ЦПС, Smart Grid и т.д.).

Объяснение несостоятельности организационных мероприятий как квинтэссенции проблемы кибербезопасности заключается в человеческом факторе (как пример, можно рассмотреть понятие фишинга, которое широко распространено в сфере кибермошенничества). Организационные мероприятия должны быть неотъемлемой частью концепции кибербезопасности, но они не могут обеспечить должной защиты энергообъекта даже от несанкционированного физического доступа на объект.