ЭКСПРЕСС-ОБСЛЕДОВАНИЕ ПРОЦЕССОВ ОБЕСПЕЧЕНИЯ ИНФОРМАЦИОННОЙ БЕЗОПАСНОСТИ В АСУ ТП ЭЛЕКТРИЧЕСКИХ ПОДСТАНЦИЙ

Барановский О.К., Ладохо Е.П.

Открытое акционерное общество «АГАТ-системы управления» - управляющая компания холдинга «Геоинформационные системы управления»

Минск, Беларусь

Аудит как форма независимой оценки ИБ

Внешняя экспертная оценка текущего состояния информационной безопасности (далее – ИБ), заключающаяся в:

- проверке выполнения требований законодательства;
- сравнении мер защиты информации и обеспечения ИБ с лучшими практиками;
- выработке рекомендаций по их улучшению.

Направления обследования

1) анализ содержания документированной информации (в том числе проектной) об объекте информационной инфраструктуры (далее – ОИИ), процессах и реализованных мерах защиты информации (далее – ЗИ) и обеспечения ИБ на соответствие законодательству;

2) поиск характеристик (уязвимостей) активов ОИИ и их рассмотрение на предмет возможной эксплуатации;

3) оценка соответствия применяемых мер и средств ЗИ установленным требованиям по ЗИ и обеспечению ИБ;

4) тестирование ОИИ на предмет возможной эксплуатации уязвимостей активов ОИИ нарушителем.

Технические мероприятия обследования ИБ

- выявление уязвимостей программного обеспечения (далее – ПО) и сетевых служб;
- контроль устранения ранее выявленных уязвимостей;
- контроль выполнения требований ЗИ, в том числе анализ настройки программных и программно-аппаратных средств ОИИ, средств ЗИ на соответствие проектной, конструкторской и эксплуатационной документации, ЛПА в области ЗИ и обеспечения ИБ;
- внешнее и (или) внутреннее тестирование на проникновение, тестирование устойчивости к атакам типа «отказ в обслуживании».

Оценка уровня зрелости организации

- Подразделение или лицо, ответственное за ЗИ
- Политика ИБ
- Инвентаризация активов ОИИ
- Модель угроз ИБ
- Управление доступом, использование встроенных механизмов и средств ЗИ
- Мониторинг ИБ и реагирование на инциденты ИБ
- Информирование и обучение персонала

НПА, ТНПА и локальные акты

- Приказ ОАЦ от 20 февраля 2020 г. № 66 «О мерах по реализации Указа Президента Республики Беларусь от 9 декабря 2019 г. № 449»
- Приказ Министерства энергетики Республики Беларусь от 18.03.2015 № 50
- Приказ ГПО «Белэнерго» 30.10.2023 № 286 «Об утверждении изменений к стандартам ГПО «Белэнерго»»
- Приказ ОАЦ от 25 июля 2023 г. № 130 «О мерах по реализации Указа Президента Республики Беларусь от 14 февраля 2023 г. № 40»
- СТБ ISO/IEC 27001-2016 Информационные технологии. Методы обеспечения безопасности. Системы менеджмента информационной безопасности. Общие требования
  (СТБ ISO/IEC/ПР1 27001 Информационная безопасность, кибербезопасность и защита конфиденциальности. Системы менеджмента информационной безопасности. Требования)

Изменение № 3 в СТП 33243.01.216-16

ИЗМЕНЕНИЕ № 3 СТП 33243.01.216-16

СТАНДАРТ ГПО «БЕЛЭНЕРГО»
Подстанции электрические напряжением 35 кВ и выше
Нормы технологического проектирования

Введено в действие приказом государственного производственного объединения электроэнергетики «Белэнерго» (ГПО «Белэнерго») от __.__.2023 № __.

Дата введения 2023-__-__

1. Содержание. Дополнить абзацем:
«23 Информационная безопасность».
2. Содержание. Дополнить абзацем:
«Приложение В (обязательное) Состав работ по защите информации при разработке ИС».

«23 Информационная безопасность
23.1 Общие требования
23.1.1 В соответствии с требованиями нормативных правовых актов Республики Беларусь [32] и [33] должны разрабатываться:
– СЗИ, отвечающая требованиям [29], для ИС, предназначенных для непосредственного управления оборудованием ПС;
– СИБ, отвечающая требованиям [31], для ПС, имеющих три и более линий электропередачи напряжением 220 кВ и более или ИС которых непосредственно управляют оборудованием ПС напряжением 220 кВ и более.

23.1.3 Исходные данные для проектирования СЗИ (СИБ) должны предоставляться разработчику в виде утвержденных руководителем организации – владельца ПС документов и включать:
– действующую Политику информационной безопасности организации – владельца ПС (КВОИ) [29];
– сведения о категориях обрабатываемой в ИС информации и перечни защищаемой информации по каждой из категорий [32];
– копию акта отнесения ИС к классу типовых ИС согласно приложению 2 к [29] либо копию приказа (распоряжения) руководителя государственного органа или его уполномоченного заместителя об отнесении ИС к КВОИ;
– перечень аварийных установившихся режимов ПС, которые могут быть инициированы путем несанкционированного (ошибочного) воздействия на технические средства, ПО и обрабатываемую в ИС ПС информацию;
– правила разграничения доступа персонала ПС к информационным активам ИС ПС [32];
– перечень и характеристики источников несанкционированных воздействий на информационные активы ИС ПС, оформленные в виде модели угроз или модели нарушителя.

Разъяснение регулятора по приказу ОАЦ № 60

Вопрос-ответ

Какие требования законодательства в сфере обеспечения кибербезопасности предъявляются к организациям, не упомянутым в Указе № 40 или постановлении Правительства № 120?

Таким организациям следует обеспечить соблюдение требований по кибербезопасности объектов информационной инфраструктуры государственных органов и иных организаций, определенных приказом Оперативно-аналитического центра при Президенте Республики Беларусь от 25 июля 2023 г. № 130 «О мерах по реализации Указа Президента Республики Беларусь от 14 февраля 2023 г. № 40» (приложение 4 к приказу).

При этом:

- данные требования вступили в силу с 17 августа 2023 г.;
- они рапространяются не только на государственные органы и организации, но и на иные организации, вне зависимости от их организционно-правовой формы;
- к объектам информационной инфраструктуры относятся критически важные объекты информатизации, информационные сети, информационные системы, информационные ресурсы и иные совокупности технических средств, систем и технологий создания, преобразования, передачи, использования и хранения информации, принадлежащие государственным органам и иным организациям на праве собственности, хозяйственного ведения, оперативного управления или на ином законном основании, за исключением объектов информатизации, предназначенных для обработки информации, содержащей государственные секреты.

Анализ документированной информации

- «Категории» информации: «общедоступная информация с регламентированным доступом», «конфиденциальная», «ограниченного доступа», «для внутреннего пользования»
- Содержание ЛПА по ЗИ состоит из выдержек НПА и ТНПА, неадаптированного текста из интернет-источников, без учета специфики АСУ ТП
- …

Поиск характеристик (уязвимостей) активов ОИИ

- анализ архитектуры и активов АСУ ТП, ее внутренних и внешних информационных потоков, в том числе наличия пользователей внутри и снаружи КЗ. Эксперт собирает сведения для актуализации схемы локальной вычислительной сети (далее – ЛВС), проводит инвентаризацию сетевого оборудования, средств маршрутизации и межсетевого экранирования, выясняет, изолирована ли сеть АСУ ТП, выявляет наличие соединений АСУ ТП с корпоративным сегментом, наличие линий связи, выходящих за пределы ПС
- обследуются автоматизированные рабочие места (далее – АРМ) и серверы: проверяются версии операционных систем (далее – ОС), их настройки, лицензии на ПО, сертификаты, группы пользователей, выясняется, установлены ли средства ЗИ.

Оценка мер и средств ЗИ требованиям ЗИ и ИБ

Выборочная проверка выполнения положений НПА, локальных актов и ЛПА в объектах АСУ ТП, средствах ЗИ:

- настроек аудита событий ИБ в ОС, средствах ЗИ и прикладном ПО;
- настроек средств ЗИ и локальных политик безопасности согласно эксплуатационной документации и ЛПА;
- реализации мер контроля использования съемных машинных носителей информации;
- выполнения мер по созданию резервных копий согласно установленному порядку и расписанию;
- должного документирования реализуемых мер ЗИ и обеспечения ИБ, в том числе в ходе внутреннего аудита системы ИБ КВОИ;
- соблюдения персоналом ЛПА (в форме выборочного опроса).

Недостатки

- фактическое состояние ОИИ не задокументировано, имеются неучтенные активы;
- настройки управления внешними и внутренними информационными потоками, антивирусным ПО и контролем подключения съемных носителей информации не документированы, а, следовательно, не проверяются в процессе процедур внутреннего аудита;
- отсутствует перечень событий ИБ, подлежащих аудиту, не настроен мониторинг событий средствами ОС;
- в ходе процедур внутреннего аудита ИБ фиксируется факт регламентации мер ЗИ в ЛПА без фактической проверки их выполнения: не проверяются журналы аудита событий ИБ, журналы учета съемных носителей информации и выполненных мероприятий по резервному копированию, настройки парольной политики ОС, соответствие фактических настроек средств ЗИ содержанию ЛПА и иных документов;

Недостатки

- поиск уязвимостей в ПО не ведется, так как работы по ЗИ выполняются силами владельца ОИИ, отсутствуют необходимые технические средства и компетенции у работников по поиску и безопасной установке патчей и обновлений (либо принятия компенсирующих мер ЗИ), а специализированные организации не привлекаются в целях экономии средств;
- отсутствует перечень информационных ресурсов, ПО, настроек, файлов конфигураций, журналов, подлежащих резервному копированию;
- не ведется учет создания резервных копий критичных активов;
- при привлечении подрядчиков для модернизации (обслуживания) ТС и ПО не предъявляются требования к обеспечению ИБ при проведении ими работ;

Недостатки

- не обрабатываются уязвимости цепочек поставок – отсутствуют процедуры тестирования обновлений прикладного ПО ОИИ;
- работники подразделений, осуществляющих мониторинг событий ИБ и реагирующих на инциденты ИБ, не имеют необходимых средств автоматизации, находятся территориально удаленно и прибыть на объект могут только через несколько часов;
- при внесении изменений и дополнений в меры ЗИ и обеспечения ИБ, документация каждый раз выпускается в новой редакции (в том числе формуляры КВОИ), причины и обоснование вносимых изменений не документируются.

Спасибо за внимание!