Что нужно для разработки программы компьютерной безопасности

Василики Тафили и Трент Нельсон

Объекты, на которых используется ядерный или иной радиоактивный материал и ведется соответствующая деятельность, входят в состав критически важной инфраструктуры, на которой необходимо обеспечивать высокий уровень ядерной и физической безопасности. Применяя комплексный и инициативный подход к компьютерной безопасности, организации могут защитить активы чувствительной информации и компьютерные системы на этих объектах. МАГАТЭ рекомендует практиковать подход к компьютерной безопасности, заключающийся в том, что государства устанавливают требования к национальной стратегии или политике и способствуют обеспечению конфиденциальности и защиты чувствительной информации и компьютерных систем, связанных с физической защитой, ядерной безопасностью, учетом и контролем ядерного материала. Эти требования могут также быть оформлены в виде национальных регулирующих положений, которые предусматривают разработку и внедрение программы обеспечения компьютерной безопасности (ПКБ)*.

ПКБ — это всеобъемлющая структура, включающая ключевые элементы эффективного плана осуществления политики и процедур компьютерной безопасности, которые будут использоваться на протяжении всего срока эксплуатации ядерной установки или установки с радиоактивными источниками. Ее целью является защита активов чувствительной информации и компьютерных систем, критически важных для поддержания функций ядерной и физической безопасности, от киберугроз для смягчения последствий кибератак.

Национальная стратегия

Комплексная и эффективная стратегия компьютерной безопасности требует системного подхода, который объединяет различные элементы, включая нормативные акты, программы, меры защиты и безопасности и потенциал реагирования для поддержания национальных режимов физической ядерной безопасности.

Регулирующие положения

Эффективные регулирующие положения обеспечивают правовую основу для защиты чувствительных компьютерных систем и наличие у организаций ПКБ с надлежащими механизмами контроля.

Ключевые элементы ПКБ

Функции и обязанности

Организационные функции и обязанности, а также структура подотчетности принципиально важны для эффективного управления, особенно в случае критической инфраструктуры. Четкое понимание организационной иерархии, распределения полномочий и структуры отчетности необходимы для эффективного и результативного сотрудничества и синергетического взаимодействия в рамках ПКБ.

Управление рисками, контроль факторов уязвимости и обеспечение соответствия нормативным требованиям

Управление рисками в области компьютерной безопасности включает оценку факторов уязвимости и потенциальных последствий, связанных с чувствительными цифровыми активами и компьютерными системами, для внедрения средств компьютерной безопасности на основе дифференцированного подхода с целью защиты от кибератак. Уровень применяемых мер безопасности должен быть соизмерим с уровнем угроз для защищаемой информации и/или компьютерных систем. Организации могут корректировать уровень мер безопасности, необходимых для снижения риска, с учетом возможных последствий реализации рисков или угроз.

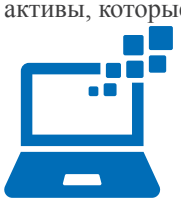
Разработка мер безопасности и управление ими

Структура системы компьютерной безопасности — важнейший аспект защиты от киберугроз. Основные принципы построения такой системы — дифференцированный подход и глубокоэшелонированная защита, когда противодействие атакам ведется на

нескольких рубежах безопасности. Требования к физической безопасности также должны выполняться на всех этапах процесса разработки системы, в том числе сторонними организациями, которые должны соблюдать четко сформулированные принципы и договоренности для обеспечения последовательности и эффективности мер физической безопасности.

Управление цифровыми активами

Эффективное обеспечение компьютерной безопасности сложно представить без системного подхода к составлению полного перечня всех функций, активов и систем объекта, включая чувствительные цифровые активы, которые необходимы для защиты ядерной



деятельности и для обеспечения безопасного и надежного использования ядерного и другого радиоактивного материала. Такой перечень также дает представление о потоках данных и взаимосвязях, которое необходимо организации для организации контроля доступа, резервного копирования и других мер безопасности, направленных на защину активов от саботажа или хищения.

Процедуры обеспечения физической безопасности

Оперативная политика и процедуры обеспечения физической ядерной безопасности распределяют ответственность за предотвращение хищения, саботажа или несанкционированного использования ядерного материала и установок. Эти процедуры предусматривают жесткий контроль доступа к конфиденциальной информации и активам, а также отбор и соответствующее обучение лиц, имеющих доступ.

Управление кадрами

Особое значение при управлении кадрами в ядерной промышленности придается благонадежности

сотрудников, их квалификации и обучению. Оценка благонадежности проводится для того, чтобы убедиться: на сотрудника можно положиться, он компетентен и не вовлечен в какие бы то ни было конфликты интересов, которые могут поставить под угрозу ядерную безопасность или физическую ядерную безопасность. Укомплектование квалифицированными и благонадежными кадрами имеет решающее значение для обеспечения ядерной и физической безопасности.

**Более подробные сведения включены в публикацию «Computer Security Techniques for Nuclear Facilities» («Методы обеспечения компьютерной безопасности для ядерных установок») (IAEA Nuclear Security Series No. 17-T (Rev. 1)).*