# Разработка системы менеджмента информационной безопасности критически важных объектов энергетической отрасли

**М.Н. Бобов, Д.Г. Горячко, А.А. Обухович (ОАО «АГАТ-системы управления»)**

*ОАО «АГАТ-системы управления» — ведущее в Беларуси предприятие по созданию автоматизированных систем управления общего и специального назначения, аппаратно-программных комплексов и технических средств, в том числе средств связи и передачи данных, вычислительной техники, контрольно-измерительных приборов, систем жизнеобеспечения и электропитания. Основной вид его деятельности — создание и поставка систем управления в интересах Министерства обороны Республики Беларусь, других министерств и ведомств, зарубежных заказчиков, в том числе из стран ЕС.*

*При разработке систем управления значительное внимание уделяется вопросам информационной и кибербезопасности. В связи с важностью данной задачи ОАО «АГАТ-системы управления» разработало национальную систему менеджмента информационной безопасности критически важных объектов.*

*В статье представлены основные положения этой концепции на примере энергетической отрасли.*

*Ключевые слова: система менеджмента информационной безопасности, критически важные объекты информатизации, АСУТП.*

Система менеджмента информационной безопасности (СМИБ) является частью общей системы управления бизнес-процессами организации (предприятия) и включает организационную структуру и комплект документов, регламентирующих ее деятельность. СМИБ представляет собой модель для создания, внедрения, функционирования, мониторинга, анализа, поддержки и совершенствования системы обеспечения информационной безопасности критически важных объектов информатизации (КВОИ), к которым относятся объекты энергетической отрасли.

Необходимость разработки СМИБ критически важных объектов информатизации в Республике Беларусь определяется ТКП 483–2013 «Информационные технологии и безопасность. Безопасная эксплуатация и надежное функционирование критически важных объектов информатизации. Общие требования», введенным в действие приказом Оперативно-аналитического центра при Президенте Республики Беларусь от 17.07.2013 N 47.

Структура СМИБ и требования к ее реализации определены СТБ ISO/IEC 27001-2011 «Информационные технологии. Методы обеспечения безопасности. Системы менеджмента информационной безопасности. Требования» и СТБ ISO/IEC 27002-2012 «Информационные технологии. Методы обеспечения безопасности. Кодекс практики для менеджмента информационной безопасности». Основная задача, которая стоит перед разработчиком – определить типовую организационную структуру и необходимый и достаточный комплект документов СМИБ для КВОИ энергетической отрасли. Формулировка основной задачи определяет необходимые принципы, которым должна соответствовать СМИБ, а именно:

— согласованность СМИБ с существующей структурой управления в энергетике на всех уровнях;

— необходимость и достаточность документов для подтверждения соответствия СМИБ требованиям СТБ ISO/IEC 27001-2011;

— соответствие области применения документов СМИБ уровню их утверждения.

Типовая структура управления предприятиями энергетической отрасли представлена на рис. 1.

Верхний уровень организационной структуры СМИБ составляют руководство областной организации энергетической отрасли (Облэнерго) и руководители предприятий — владельцев КВОИ, входящих в ее структуру.

Иерархия функций по управлению безопасностью в приведенной организационной структуре (рис. 1) распределяется следующим образом:

- руководство Облэнерго;
- ответственный за обеспечение информационной безопасности;
- руководители предприятий;
- подразделение технической защиты информации;
- администраторы защиты информации АСУТП КВОИ;
- персонал КВОИ.


*Рис. 1. Типовая структура управления предприятиями энергетической отрасли*

Руководство Облэнерго должно взять на себя ответственность за:

— принятие стратегических решений по вопросам обеспечения защиты информации в организации;

— координацию действий предприятий — владельцев КВОИ, входящих в структуру организации, при


*Рис.2. Организационная структура обеспечения информационной безопасности КВОИ*

планировании и выполнении мероприятий по разработке и внедрению документов СМИБ;

— утверждение основополагающих документов СМИБ;

— выделение соответствующих материальных и кадровых ресурсов для обеспечения функционирования систем защиты информации КВОИ;

— организацию обучения и повышения квалификации специалистов КВОИ в сфере информационной безопасности.

Руководители предприятий — владельцев КВОИ организуют работы и несут ответственность за разработку и внедрение документов СМИБ.

Второй уровень организационной структуры СМИБ составляет подразделение технической защиты информации организации, которое обеспечивает методическое руководство, координацию разработки и внедрения документов СМИБ на предприятиях — владельцах КВОИ.

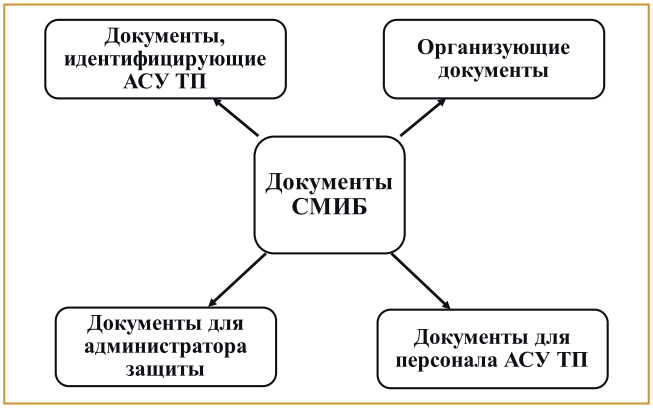


*Рис.3. Комплект документов СМИБ организации*

Нижний уровень организационной структуры составляют администраторы защиты информации КВОИ.

Организационная структура обеспечения информационной безопасности КВОИ в организации энергетической отрасли приведена на рис. 2.

Комплект документов СМИБ организации можно условно разделить на следующие категории:

— организующие документы;

— документы, регламентирующие процессы;

— документы для персонала.

Структура документов, необходимых и достаточных для функционирования СМИБ, приведена на рис. 3.

Организующие документы, утверждаемые руководством Облэнерго, включают:

— политику информационной безопасности организации;

— регламент функционирования СМИБ КВОИ организации;

— положение по разделению информационных ресурсов КВОИ по категориям доступа;

— правила разграничения доступа в КВОИ;

— модель угроз информационной безопасности в КВОИ;

— основные положения системы управления информационными рисками в КВОИ;

— методику оценки рисков информационной безопасности в КВОИ.

К документам, регламентирующим процессы на конкретных КВОИ, относятся:

— инструкции по обеспечению защиты информации;

— инструкции о порядке применения средств защиты информации;

— программа и методики проверок СОИБ КВОИ в процессе эксплуатации;

— положение об антивирусном контроле;

— положение об использовании носителей информации;

— положение о резервном копировании информации;

— положение о гарантированном уничтожении информации с носителей;

— правила реагирования на инциденты информационной безопасности;

— порядок расследования инцидентов информационной безопасности;

— методику мониторинга среды функционирования и анализа уязвимостей.

Для персонала КВОИ разрабатываются следующие документы:

— порядок оповещения лиц, ответственных за функционирование КВОИ, при обнаружении нарушений информационной безопасности;

— инструкция по использованию информационных активов КВОИ.

### Особенности АСУТП как объекта защиты

Цель защиты информации в АСУТП — обеспечение непрерывности и неизменности технологического процесса, предотвращение угроз для жизни и здоровья людей и окружающей среды. Для достижения указанной цели требуется разработать [1,2]:

— жесткие ограничения на внедрение в процесс управления оборудованием дополнительных процессов, в том числе процессов защиты информации;

— алгоритмы реагирования на выявленные при эксплуатации инциденты информационной безопасности;

— строгую процедуру доказательства функциональной надежности АСУТП при разработке и ее контроля при эксплуатации.

Отличительной особенностью АСУТП, отнесенных впоследствии к КВОИ, разработка и внедрение которых проводилась зарубежными фирмами или собственными силами предприятий — владельцев КВОИ, является практическое отсутствие эксплуатационной документации, позволяющей однозначно идентифицировать состав технических средств, программного обеспечения и обрабатываемую информацию КВОИ. Поэтому в состав документации целесообразно включить группу документов, идентифицирующих КВОИ.

К документам, идентифицирующим КВОИ, можно отнести:

— формуляр КВОИ;

— схему электрическую функциональную КВОИ;

— описание информационных процессов КВОИ;

— реестр информационных активов КВОИ.

Создание организационной структуры СМИБ является итерационным процессом, начинающимся с поручения конкретным исполнителям подготовить «План мероприятий по созданию и внедрению СМИБ» и завершающийся утверждением комплекта документов, регулирующих процессы обеспечения информационной безопасности в организации.

Документы СМИБ определяют и регулируют следующие процессы, связанные с информационной безопасностью (ИБ) объекта энергетики:

— определение и поддержание в актуальном состоянии документации, отражающей инфраструктуру, состав технических и программных средств и реализацию информационных процессов в АСУТП;

— выполнение работ по оценке и обработке рисков информационной безопасности;

— поддержку функционирования системы информационной безопасности АСУТП;

— мониторинг, анализ, поддержку и улучшение качества ИБ.

Разработка документов СМИБ КВОИ может быть осуществлена только после проведения следующих работ:

— обследование КВОИ АСУТП;

— изучение требований законодательства Республики Беларусь и действующих технических нормативных правовых актов в области КВОИ;

— анализа исходных данных, подготовленных техническими подразделениями Облэнерго.

Предлагаемый пакет документов СМИБ может рассматриваться как основа для типового проектного решения при создании систем информационной безопасности АСУТП предприятий энергетической отрасли.

**писок литературы**


1. *Бобов М.Н., Горячко Д.Г., Обухович А.А.* // Информационно-измерительные и управляющие системы. 2016. – №4, т. 14. – С. 69-74. 2.
2. *Боб ов М.Н., Обухович А.А.* Методология оценки рисков информационной безопасности // Труды XVIII научно-практической конференции «Комплексная защита информации». Брест. 2013.



***Бобов Михаил Никитич*** *– д-р техн. наук, проф., главный специалист по защите информации,*
***Горячко Дмитрий Генрихович*** *– главный инженер,*
***Обухович Андрей Анатольевич*** *– ведущий системный аналитик ОАО «АГАТ-системы управления» – управляющая компания холдинга «Геоинформационные системы управления».*
*Контактный телефон (+375-17) 267-44-55.*
*E-mail: agat@agat.by Http:// www.agat.by*


### Всероссийский центр экстренной и радиационной медицины МЧС РФ внедрил разработанную «Газинформсервис» систему защиты информации

Работы в области обеспечения информационной и физической безопасности, выполненные компанией «Газинформсервис», позволяют обеспечить защиту персональных данных в информационных системах Центра. Развернутая компанией инфраструктура открытых ключей позволила перейти на ведение юридически значимых электронных медицинских документов за счет использования сотрудниками электронных подписей. Специалистами «Газинформсервис» были реализованы пилотные проекты ведения амбулаторных медицинских записей в безбумажном виде, а также обмена электронными листами нетрудоспособности с ФСС России на базе криптографической платформы Litoria Crypto Platform. На текущий момент эти системы находятся на этапе опытной эксплуатации.

Для автоматизации управления пропускным режимом в информационно-технологическую инфраструктуру ФГБУ ВЦЭРМ им. А. М. Никифорова МЧС России была развернута автоматизированная система заказа пропусков. Кроме того, был внедрен программно-аппаратный комплекс «Блокхост-МДЗ» для защиты персональных данных пациентов и сотрудников.

Отметим, что ФГБУ ВЦЭРМ им. А. М. Никифорова МЧС России — единственное на сегодняшний день лечебное учреждение в России, прошедшее процедуру аттестации на соответствие требованиям, предъявляемым к уровню EMRAM Stage 6 (авторитетная международная оценка, разработанная организацией HIMSS). Это стало возможным благодаря системной и слаженной работе сотрудников центра и его ключевых ИТ-подрядчиков.

*Http://www.gaz-is.ru*