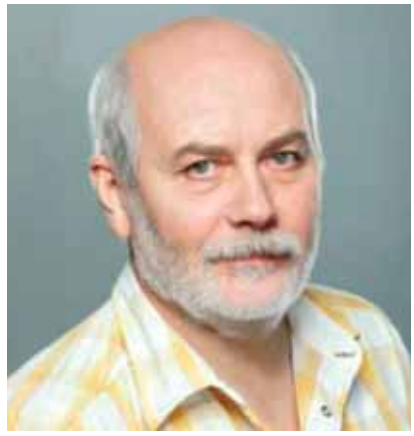
Информационная безопасность АСУТП КВО:

нормативно-правовое обеспечение, текущая ситуация

Игорь ДУША,
инженер, НИЯУ МИФИ

Александр ЗУЙКОВ,
инженер, НИЯУ МИФИ



Андрей ДУХВАЛОВ,
главный архитектор, руководитель департамента перспективных технологий, ЗАО «Лаборатория Касперского»

Проблема обеспечения информационной безопасности автоматизированных систем управления технологическими процессами (АСУ ТП) активно освещается в научных работах российских и зарубежных ученых, отчетах по исследованиям специализированных вредоносных программ и других работах [1, 2, 3, 4]. В последние два-четыре года было выпущено немало стандартов и законодательных актов [5, 6, 7], в связи с чем ориентироваться во множестве документов становится проблематично. Кроме того, при разработке систем защиты информации (СЗИ) следует учитывать требования российских законодательных актов [8, 9]. В настоящей статье выделены основные тенденции в нормативных документах, выделены особенности и недостатки документов. Материалы статьи могут быть использованы для создания единых методических рекомендаций, разработки системы защиты информации на предприятии и других работ, связанных с проблемами защиты информации (ЗИ) в АСУ ТП. Стандарты описываются в рамках заданного в статье разделения в хронологическом порядке.

Общая структура

Очевидно, что многие стандарты ничего нового в рамках принципов и подходов к информационной безопасности (ИБ) не вносят. Более того, все стандарты можно считать результатом работ по существующим методикам, учитывающим специфику АСУ ТП. Сами же стандарты можно разделить на общие стандарты, учитывающие специфику промышленных систем, в частности наличие в сети таких элементов, как промышленная система управления и разного рода датчики, и отраслевые стандарты, учитывающие особенности конкретной отрасли.

Все стандарты базируются на стандартах ISO/IEC серии 27000 (либо ISO/IEC 1799, если появились ранее 2007 г.) и используют базовые определения

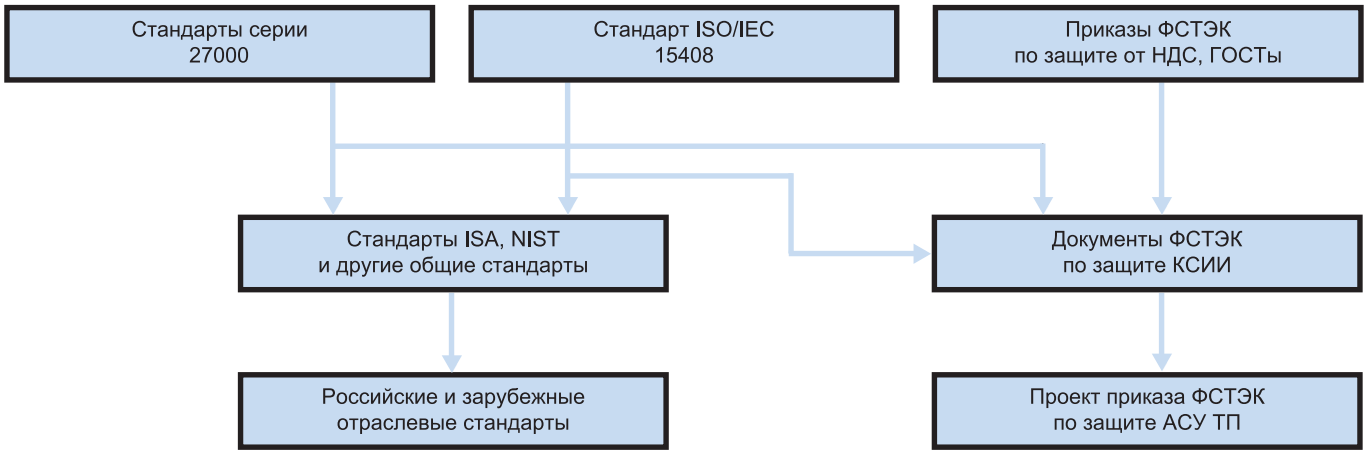


Рисунок. *Иерархия документов по защите АСУ ТП*

стандарта ISO/IEC 15408. Многие отраслевые стандарты основаны на общих стандартах ISA SP99 и NIST SP800-82. Особое внимание необходимо обратить на стандарт ISA/IEC 62443, который разрабатывается в целях создания стандарта нового поколения на базе ISA99 и серии стандартов ISO/IEC 2700x, отражающих современные подходы и практики в построении защищенных индустриальных систем [16]. Российские документы несколько отличаются от иностранных, поэтому о них будет сказано отдельно. Указанные стандарты содержат описание:

- угроз, ущерба от их реализации, их анализа;
- процесса управления системой информационной безопасности;
- правил и принципов управления персоналом, физической защиты, сетевой защиты и решения других задач ЗИ;
- отдельных частных правил и рекомендаций;
- рекомендаций в отношении использования сетевых СЗИ и защиты удаленного доступа (УД).

Основными методами, не специфичными для других областей, являются разделение сети предприятия на секторы (реализация принципа защиты в глубину) и использование промышленных диодов (однонаправленных МЭ) при обмене информацией между сетями бизнес-уровня и уровня предприятия. При этом отечественные стандарты не определяют решения таких проблем, как:

- управление промышленными беспроводными сетями;
- влияние стандартных СЗИ на временные параметры;
- обновление баз данных СЗИ;
- совмещение различных протоколов и устройств между собой.

В то же время аналогичные проблемы достаточно хорошо регулируются иностранными стандартами, например:

- промышленные беспроводные сети, управление параметрами и обновлениями системы [16, 17, 18];
- вопросы безопасности коммуникационных протоколов и систем взамодействия [19].

Мнение специалиста

Дмитрий ЯРУШЕВСКИЙ,

руководитель отдела кибербезопасности АСУ ТП, ЗАО «ДиалогНаука»:

Несмотря на недавно утвержденный приказ ФСТЭК России № 31, существенно усиливший отечественную методологическую базу по защите АСУ ТП, в российских руководящих документах все еще наблюдается острый дефицит современного подхода к вопросам защиты АСУ ТП от киберугроз. В первую очередь это проявляется в отсутствии адекватной методологии определения угроз безопасности АСУ ТП.

Например, в том же приказе № 31 фигурирует требование о проведении оценки рисков при анализе угроз ИБ. Вообще, оценка рисков – это неотъемлемая часть процесса обеспечения ИБ, как в АСУ ТП, так и в «классических» ИТ-системах. Однако методология, описывающая и регламентирующая этот процесс, в российских нормативных документах полностью отсутствует. В результате ответственным за обеспечение безопасности АСУ ТП специалистам не на что опираться при моделировании и анализе угроз безопасности. Разумеется, здесь можно (и нужно) «оглядываться» на зарубежные практики. Но, во-первых, это требует достаточно большого опыта и высокой квалификации в области ИБ, что обычно не входит в область компетенций владельцев и основных ответственных за эксплуатацию АСУ ТП. А значит, требует привлечения подрядчиков и дополнительных финансовых вливаний. Во-вторых, для владельцев АСУ ТП отсутствует мотивация в следовании рекомендациям зарубежных руководящих документов. Ведь, скажем прямо, пока еще вопросы кибербезопасности АСУ ТП часто рассматриваются как помеха технологическому процессу и дополнительная «дыра в бюджете».

Иностранные документы

Разработка нормативных документов по проблемам обеспечения ИБ АСУ в США началась в начале XXI в., сейчас насчитывается несколько десятков различных документов от нескольких организаций [10, 11]. Европейское сообщество также разработало ряд соответствующих документов, отдельно стоит упомянуть несколько стандартов: ISA SP99, NIST SP800-82, ISA/IEC 62443 (в стадии разработки и утверждения).

Подробное описание многих других документов можно найти в [10, 11].

Нормативные документы, регулирующие обеспечение ИБ АСУ ТП, делятся на два типа: общие требования безопасности и промышленные стандарты безопасности, учитывающие особенности конкретной области. Таких областей выделяется от 10 до 17. Отраслевые документы базируются на двух документах [12, 13]. Иерархия документов в общем случае изображена на рисунке.

Мнение специалиста

Станислав ШЕВЧЕНКО,
технический директор, SafenSoft:

В последнее время в информационной безопасности вопрос о стандартах ставится во главу угла. Речь идет не только о вопросах стандартизации информационной безопасности АСУ ТП, но и о любых других стандартах, связанных с информационными технологиями. Именно сейчас нужно договориться о базовых постулатах, базовых принципах, на которых мы будем работать дальше, потому что мы подходим к новой ступеньке развития ИТ-индустрии, где четко осознается: безопасность – это ключевой и неотъемлемый элемент системы. Стандартизация – очень важный момент, и говорить об этом нужно, и говорить об этом должны профессионалы. Стандарты 1980-х и 1990-х годов сейчас по большей части устарели и малоприменимы, так что необходимо создавать внутренне и взаимно непротиворечивые документы, соответствующие современным технологиям. Отдельно стоит отметить важность четкости и однозначности формулировок – каждый термин должен быть внятно определен и не допускать разночтений, позволяющих трактовать отдельные пункты в зависимости от интересов различных сторон.

Отечественные документы

В России проблеме обеспечения ИБ АСУ ТП уделяется большое внимание, о чем говорят, в частности, № 256-ФЗ «О безопасности объектов топливно-энергетического комплекса» [8]

> Главной целью защиты информации является сохранение конфиденциальности и целостности этой информации даже в ущерб ее доступности.

В рамках отраслевых стандартов, например выпущенных American Gas Association (AGA 12) или American Petroleum Institute (API 1164), можно найти угрозы, специфические для данной отрасли, с указанием степени риска и некоторые уточнения относительно СЗИ, политики ИБ.

и соответствующий документ Совета безопасности [14]. Второй документ определяет развитие ИБ АСУ ТП как области – определяются цели и задачи, а также план решения данных задач. Основной отечественный документ ФСТЭК, регулирующий правила защиты АСУ ТП, в настоящее время находится на этапе утверждения.

Базовым документом по обеспечению ИБ АС до 2007 г. в РФ был РД ФСТЭК «Автоматизированные системы. Защита от несанкционированного доступа к информации. Классификация автоматизированных систем и требования по защите информации», выпущенный в 1992 г. Данный документ актуален до сих пор, в нем описывается состав СЗИ для АС, которые обрабатывают информацию, относящуюся к государственной тайне.

Главной целью защиты информации, составляющей государственную тайну, является сохранение конфиденциальности и целостности этой информации даже в ущерб ее доступности. Об этом говорит название документа, обозначающее единственную угрозу – несанкционированный доступ к информации.

Обобщая вышесказанное, укажем основные условия, выполнение которых необходимо для защиты в соответствии с данным документом, но невозможно для АСУ:

- доступ к АС извне закрыт;
- нет системы управления ИБ, проверок и постепенного улучшения политик безопасности

Мнение специалиста

Дмитрий МОИСЕЕВ,

CISSP, руководитель практики аналитических систем компании «Астерос Информационная безопасность» (группа «Астерос»):

Основным нормативным документом по защите информации в автоматизированных системах управления производственными и технологическими процессами, действующим на территории Российской Федерации, является приказ ФСТЭК России от 14.03.2014 № 31 «Об утверждении Требований 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». Данный документ вобрал в себя все основные аспекты защиты информации в АСУ ТП, представленные в упомянутых в статье международных стандартах. На мой взгляд, это свидетельствует о серьезном подходе отечественных регуляторов к защите информации в АСУ ТП.

Стоит отметить, что в данном приказе ФСТЭК России затронуты такие направления, как анализ рисков и угроз, управление инцидентами ИБ, обеспечение непрерывности производственных и технологических процессов, а также вопросы защиты виртуальных сред и мобильных устройств. Поэтому теперь необходимо руководствоваться именно этим документом, дополняя его, при необходимости, требованиями национальных, отраслевых стандартов, а также международных стандартов в области защиты информации в АСУ ТП.

и настроек средств обеспечения ИБ;
- система защиты не предусматривает атаки со стороны внутреннего нарушителя, так как соответствующий контроль лежит на организационных методах ЗИ.

В 2007 г. был выпущен ряд документов по ЗИ в ключевых системах информационной инфраструктуры (КСИИ), отчасти касающихся защиты АСУ ТП [5, 6, 7]. Документы описывали базовую модель угроз ИБ КСИИ, методику по определению актуальных угроз, общие требования и рекомендации. Требования представлены как классическими элементами ЗИ от несанкционированного доступа (НСД), например системой управления доступом, регистрации и учета, обеспечения целостности, так и современными требованиями ИБ: применение систем обнаружения вторжений (СОВ), систем анализа защищенности, аудит безопасности и др. Однако данный документ не учитывает специфику АСУ ТП и актуальных проблем данной области, потому может применяться с некоторыми ограничениями.

В начале 2014 г. был опубликован проект приказа ФСТЭК, утверждающий ряд требований к обеспечению защиты информации в АСУ ТП на КВО. Документ решает задачи комплексного обеспечения информационной безопасности и устанавливает состав СЗИ.

Документ разработан в соответствии с современными представлениями об обеспечении ИБ предприятия, ясно формулирует и определяет требования к защите. Он содержит описание жизненного цикла как самой АСУ, так и ПО, требования к составу средств защиты в зависимости от конкретной системы, однако не включает конкретные методические указания по защите, которые должны быть раскрыты уже в следующих нормативных актах.

Заключение

На сегодняшний день выпущено немало стандартов, регулирующих область ЗИ в АСУ ТП. Многие из рекомендаций, приведенных в этих документах, есть не что иное, как применение известных всем специалистам по ИБ общемировых подходов к ЗИ, и они лишь утверждают те или иные части политики. Однако даже в этих стандартах не учтены некоторые особенности АСУ ТП по причине отсутствия подходов к решению задач ЗИ в АСУ ТП.

Стандарты АСУ ТП исторически рассматриваются в контексте надежности систем и, как правило, сертифицируются на основании систем надежности и отказоустойчивости (например, по SIL (Safety Integrity Level), FSS (Functional Safety Standards) [20]). Сегодня неотъемлемой частью общей надежности систем

Стандарты АСУ ТП исторически рассматриваются в контексте надежности систем и сертифицируются на основании систем надежности и отказоустойчивости.

становится кибербезопасность, поэтому наблюдается определенный дефицит общемировых и отечественных стандартов, направленных на унификацию рекомендаций и практик по обеспечению кибербезопасности с детальными практическими пошаговыми процедурами реализации, проверки и оценки состояния защищенности в соответствии с моделью угроз конкретного критически важного объекта. Разрабатываемый IEC 62443 – очень важный шаг в нужном направлении. Современные отраслевые специализированные стандарты также начинают уделять внимание вопросам кибербезопасности с учетом специфики объектов конкретной отрасли. ■

Современные отраслевые специализированные стандарты также начинают уделять внимание вопросам кибербезопасности с учетом специфики объектов конкретной отрасли.

Литература

1. *Гордейчик С. Безопасность промышленных систем в цифрах. М.: Positive technologies, 2012.*
2. *Кондратенко А. ИБ в ключевых системах информационной инфраструктуры. М.: Connect. 2013. № 9.*
3. *Гарбук С.В., Комаров А.А., Салов Е.И. Аналитический отчет «Обзор инцидентов информационной безопасности АСУ ТП зарубежных государств». М.: НТЦ «Станкинформзащита», 2010.*
4. *Гаврилов В. Фундамент безопасности АСУ ТП: от правовых основ до особых методик. М.: Connect. 2013. № 9.*
5. *Базовая модель угроз безопасности информации в ключевых системах информационной инфраструктуры (утв. ФСТЭК России 18.05.2007).*
6. *Методика определения актуальных угроз безопасности информации в ключевых системах информационной инфраструктуры (утв. ФСТЭК России 18.05.2007).*
7. *Рекомендации по обеспечению безопасности информации в ключевых системах информационной инфраструктуры (утв. ФСТЭК России 19.11.2007).*
8. *Федеральный закон № 256-ФЗ. О безопасности объектов топливно-энергетического комплекса // РГ: Федеральный выпуск № 5537 26.07.2011.*
9. *Федеральный закон № 116-ФЗ. О промышленной безопасности опасных производственных объектов. Приложение 1 // РГ: Федеральный выпуск № 3831 27.07.2005.*
10. *Sommestad T. SCADA system cyber security. A comparison of standards, Power and Energy Society General Meeting, 2010 IEEE, 8 p.*
11. *Лукацкий А. Обзор мировых стандартов ИБ АСУ ТП и советы по их применимости в российских условиях // Материалы конференции INFOBEZ-EXPO.*
12. *Critical infrastructure sectors. [Электронный ресурс] Режим доступа: https://www.dhs.gov/critical-infrastructure-sectors.*
13. *Canada Critical Infrastructure. [Электронный ресурс] Режим доступа: http://www.publicsafety.gc.ca/ cnt/ntnl-scrt/crtcl-nfrstrctr/index-eng.aspx*
14. *Основные направления государственной политики в области обеспечения безопасности автоматизированных систем управления производственными и технологическими процессами критически важных объектов инфраструктуры Российской Федерации. [Электронный ресурс] Режим доступа: http://www.scrf.gov.ru/documents/6/113.html*
15. *Проект «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». [Будет доступен после утверждения на сайте http://fstec.ru/].*
16. *ISA/IEC 62443 Security for Industrial Automation and Control Systems, Draft: http://isa99.isa.org/Documents/Drafts/*
17. *Guide to Industrial Control Systems (ICS) Security SP800-82: http://nvlpubs.nist.gov/nistpubs/SpecialPublications/NIST.SP.800-82r1.pdf*
18. *NIST 800-48 Guide to Securing Legacy IEEE 802.11 Wireless Networks: http://csrc.nist.gov/publications/nistpubs/800-48-rev1/SP800-48r1.pdf*
19. *IEC 62351 Security Standards.*
20. *SIL/FSS Standards: ANSI/ISA 84; Safety Integrity Level/Functional Safety Standards (IEC 61508/IEC 61511).*