УДК 681.5

Нормативно-правовое регулирование информационной безопасности автоматизированных систем управления технологическими процессами

Т.Ю. Кирилина, д.соц.н., заведущий кафедрой гуманитарных и социальных дисциплин,
Государственное бюджетное образовательное учреждение высшего образования Московской области «Технологический университет», г. Королев, Московская область,
Е.Н. Горбанева, методист, Центр Педагогического Мастерства, г. Москва,
А.В. Познякевич, младший менеджер по развитию бизнеса, Лаборатория Касперского, г. Москва

На сегодняшний день защита автоматизированных систем управления технологическими процессами в Российской Федерации – одна из самых важных тем в области информационной безопасности. Число киберугроз на промышленные системы увеличиваются, что имеет критическое значение для экологической, социальной и макроэкономической составляющей государства.

Кибербезопасность, информационные технологии, операционные технологии, ИТ-безопасность.

Legal and regulatory framework of Information security of automated process control systems

T.Yu. Kirilina, Doctor of sociological sciences, the head of the Department of Humanities and social Sciences,
State Educational Institution of Higher Education Moscow Region «University of technology», Korolev, Moscow region,
E.N. Gorbaneva, The methodologist in the Center of Pedagogical Skills of Moscow,
A.V. Poznyakevich, The junior business development manager in Kaspersky Lab, Moscow

Nowadays protection of automated process control systems in the Russian Federation is one of the most important problems in the field of information security. Number of cyberthreats is increasing dramatically that has critical value for an ecological, social and macroeconomic component of the state.

Cybersecurity, information technology, operating technology, IT-security.

На сегодняшний день защита автоматизированных систем управления технологическими процессами (далее – АСУ ТП) в Российской Федерации (далее – РФ) – одна из самых важных тем и становится не только своеобразным трендом среди промышленных предприятий, но и регламентируется государством [3; 4]. Следует отметить, что специалисты в области информационной безопасности погружены в тему обеспечения безопасности конфиденциальной информации и персональных данных достаточно давно. Вопросы, касающиеся защиты информации, почти во всех отраслях определены, а также выработаны некоторые принципы и подходы к построению систем информационной безопасности.

Проблема обеспечения информационной безопасности автоматизированных систем управления технологическими процессами активно освещается в научных работах российских и зарубежных ученых, отчетах по исследованиям специализированных вредоносных программ и других работах. Целесообразно отдельно выделить достаточно полный и проработанный аналитический отчет Гарбука С.В., Комарова А.А. и Салова Е.И. «Обзор инцидентов информационной безопасности АСУ ТП зарубежных государств», выпущенный в 2010. В своей работе я буду также опираться на статью Гаврилова В. «Фундамент безопасности АСУ ТП: от правовых основ до особых методик», аналитический отчет Гордейчика С. «Безопасность промышленных систем в цифрах» и отчеты специалистов центра реагирования на инциденты кибербезопасности (далее – ICS-CERT). Также следует отметить масштабное исследование «Лаборатории Касперского» «ICS and their online availability» в 2016 году. Кроме того, в этом же году «Лаборатория Касперского» открыла собственный, первый в РФ ICS CERT, который направлен на координацию действий производителей систем автоматизации, владельцев и операторов промышленных объектов, исследователей информационной безопасности при решении задач защиты промышленных предприятий и объектов критически важных инфраструктур [9].

Следует заметить, что все же остается немало вопросов в части защиты систем АСУ ТП на промышленных предприятиях и предприятиях топливно-энергетического комплекса. Немаловажную роль в этом играет то, что защита таких систем до недавнего времени в РФ была вне зоны внимания специалистов по информационной безопасности и государственных регуляторов [1, с.3].

Внимание к данной проблеме было вызвано несколькими факторами: Первый – произошедшие и происходящие в настоящий период инциденты (вирус-червь Stuxnet, взлом серверов и кража информации OaSyS SCADA Telvent (Schneider Electric) и другие инциденты). Второй – закончился долгий период отсутствия внимания к проблеме со стороны отечественных регуляторов. После выпуска документа «Система признаков критически важных объектов» в 2005 г. наступала семилетняя пауза, которая была прервана Советом Безопасности РФ. В 2012 г. был выпущен документ «Основные направления государственной политики в области обеспечения безопасности автоматизи-

рованных систем управления производственными и технологическими процессами критично важных объектов инфраструктуры Российской Федерации». После этого государственные регуляторы начали уделять достаточно пристальное внимание вопросам защиты АСУ ТП.

Нормативно-правовое регулирование ИБ АСУ ТП

Проработка вопросов по подготовке нормативных документов, касающихся обеспечения информационной безопасности АСУ ТП, впервые началась в США в начале XXI века. На сегодняшний день можно перечислить несколько десятков различных документов от ряда организаций. Европейское сообщество тоже не оставалось в стороне и подготовило ряд соответствующих документов из которых целесообразно упомянуть следующие: ISA SP99, NIST SP800-82, ISA/ IEC 62443.

Нормативные документы, которые призваны регулировать обеспечение ИБ АСУ ТП, можно разделить на два типа: общие требования безопасности и промышленные стандарты безопасности, которые учитывают особенности конкретной области. Подобных областей можно выделить порядка пятнадцати [3, с.4].

В Российской Федерации действуют не меньше тридцати документов, которые в разной степени затрагивают и регламентируют информационную защиту АСУ ТП. Иерархия документов в общем случае представлена на рисунке 2.

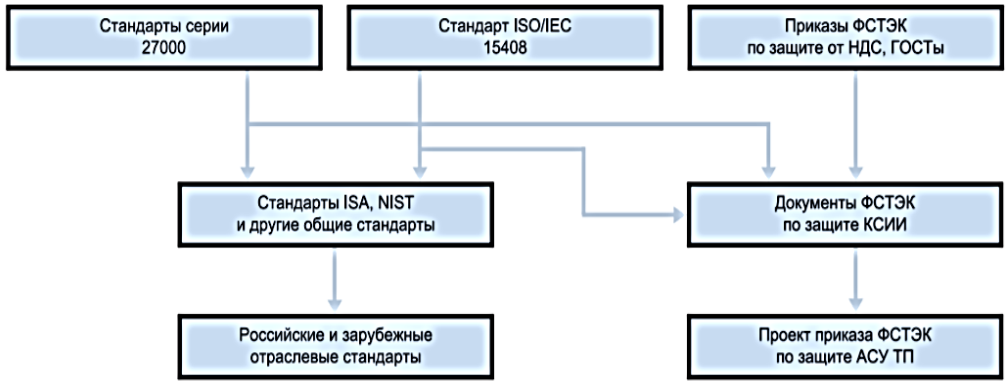

Рисунок 2 – Иерархия документов, регламентирующих ИБ АСУ ТП
Источник: Обеспечение информационной безопасности АСУ ТП // bis-expert.ru/articles/49501

Из категории документов, регламентирующих информационную защиту автоматизированных систем управления технологическими процессами в России, целесообразно выделить четыре документа Федеральной службы по техническому и экспортному контролю (далее – ФСТЭК): «Базовая модель угроз безопасности информации в КСИИ», «Методика определения актуальных угроз безопасности информации в КСИИ», «Общие требования по обеспечению безопасности информации в КСИИ», «Рекомендации по обеспече-

нию безопасности информации в КСИИ». Перечисленные документы распространялись только под грифом «Для служебного пользования (ДСП)». Следует отметить, что именно с момента выпуска данных четырех документов в 2007 году, база документов в сфере защиты АСУ ТП начала развиваться более предметно.

Новым витком развития нормативной базы можно считать принятие в 2011 г. Федерального закона №256-ФЗ «О безопасности объектов топливно-энергетического комплекса (ТЭК)», который обязывал к проектировке и внедрению систем обеспечения информационной безопасности объектов ТЭК. Данный закон обязывал субъектов топливно-энергетической отрасли использовать системы защиты информации от неправомерного доступа, уничтожения, модифицирования, блокирования или других неправомерных действий.

Следующей стадией развития нормативно-правовой базы можно считать принятие приказа ФСТЭК России №31 в 2014 г. Данный документ содержит ряд требований к обеспечению информационной безопасности АСУ ТП на критически важных объектах (далее – КВО), а также потенциально опасных или представляющих повышенную опасность объектах. Можно отметить, что на сегодняшний день с практической точки зрения именно этот документ является главенствующим в вопросе обеспечения ИБ АСУ ТП. Документ был разработан в соответствии со сложившимися представлениями об обеспечении информационной безопасности предприятия, ясно формулировал и определял требования к защите информации. 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 ИБ. Нормативные документы ФСТЭК определяют, что состав и содержание мер защиты АСУ ТП должен определять владелец или оператор системы в зависимости от ее класса защищенности, структурно-функциональных характеристик АСУ ТП, реализуемых информационных технологий, особенностей функционирования защищаемого технологического процесса и от актуальных угроз и целей защиты. В состав приказа ФСТЭК № 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», входят следующие блоки требований:

- идентификация и аутентификация субъектов доступа и объектов доступа;
- управление доступом субъектов доступа к объектам доступа;
- ограничение программной среды;
- защита машинных носителей информации, на которых хранится и (или) обрабатывается защищаемая
- информация;
- регистрация событий безопасности;

- антивирусная защита;
- обнаружение (предотвращение) вторжений;
- контроль (анализ) защищенности защищаемой информации;
- обеспечение целостности АСУ ТП и защищаемой информации;
- обеспечение доступности защищаемой информации;
- защита среды виртуализации;
- защита технических средств;
- защита АСУ ТП, ее средств, систем связи и передачи данных;
- безопасная разработка прикладного и специального программного обеспечения разработчиком;
- управление обновлениями программного обеспечения;
- планирование мероприятий по обеспечению защиты информации;
- обеспечение действий в нештатных (непредвиденных) ситуациях;
- информирование и обучение пользователей;
- анализ угроз безопасности информации и рисков от их реализации;
- выявление инцидентов и реагирование на них;
- управление конфигурацией информационной системы и ее системы защиты [6, с. 31-42].

Следует также отметить утверждение 5 декабря 2016 года Президентом Российской Федерации новой доктрины информационной безопасности. Предыдущая доктрина была утверждена еще в 2000-м году и являлась откровенно устаревшей. Доктрина является документом стратегического планирования в сфере обеспечения информационной безопасности. Согласно утвержденной доктрине «обеспечение устойчивого и бесперебойного функционирования информационной инфраструктуры, в первую очередь критической информационной инфраструктуры Российской Федерации (далее – критическая информационная инфраструктура) и единой сети электросвязи Российской Федерации, в мирное время, в период непосредственной угрозы агрессии и в военное время» является национальным интересом в информационной сфере [5]. Также следует обратить внимание на проект ФЗ «О безопасности критической информационной инфраструктуры Российской Федерации» от 6 декабря 2016 года. В проекте говорится о повышении уровня защищенности объектов критической информационной инфраструктуры. Можно утверждать, что Президент Российской Федерации в последнее время уделяет довольно пристальное внимание вопросу защиты критических инфраструктур. Еще одно свидетельство тому его недавнее послание Федеральному собранию, в котором говорится: «Необходимо укреплять защиту от киберугроз, должна быть значительно повышена устойчивость всех элементов инфраструктуры, финансовой системы, государственного управления. Предлагаю запустить масштабную системную программу развития экономики нового технологического поколения, так называемой цифровой экономики. В её реализации будем опираться именно на российские компании, научные, исследовательские и инжиниринговые центры страны. Это вопрос национальной безопасности и техно-

логической независимости России, в полном смысле этого слова – нашего будущего» [5].

Таким образом, на данный момент у специалистов в области информационной безопасности промышленных предприятий имеется в распоряжении достаточно полная и применимая на практике база нормативных документов, а также поддержка государства в вопросе обеспечения безопасности критических инфраструктур. Следование их требованиям вкупе со знанием лучших отраслевых практик, описанных в зарубежных документах, позволит обеспечивать киберзащиту производственных и технологических процессов.

Для понимания различий отечественного и западного подходов в вопросе регулирования безопасности автоматизированных систем, проведем сравнение 31-й приказа ФСТЭК и стандарта NIST SP 800-82. Первое, что необходимо отметить – это то, что при разработке 31 Приказа специалисты ФСТЭК определённо изучали зарубежные стандарты и рекомендации по обеспечению безопасности автоматизированных систем управления, в том числе и достаточно авторитетный стандарт NIST SP 800-82. Следовательно, можно утверждать, что российский документ хорошо согласован с международной нормативной базой. Тем не менее, имеются и серьезные различия в подходах.

Стоит подчеркнуть, что NIST SP 800-82 является скорее не стандартом, а расширенным набором рекомендаций по комплексному обеспечению безопасности индустриальных систем, который также содержит методические наработки практиков в данной области. В свою очередь, Приказ ФСТЭК № 31 – это достаточно формализованный документ, который создавался отчасти по аналогии с Приказами ФСТЭК № 17 и № 2.

В Приказе № 31 работа по обеспечению защиты информации АСУ ТП разделяется на пять этапов:

- формирование требований (в том числе определение уровня значимости системы, необходимого класса защищенности, возможных угроз и требований к системе защиты);
- разработка системы защиты на основе сформулированных требований;
- внедрение системы;
- обеспечение защиты в процессе эксплуатации системы;
- обеспечение защиты при выводе системы из эксплуатации.

Стандарт NIST в свою очередь не выдвигает каких-либо формальных требований, а лишь предлагает набор методик и практических рекомендаций. Он содержит:

- предметные рекомендации, дающие представление о том, с чего следует начать и как наиболее эффективно построить систему защиты в целом;
- упрощенные модели злоумышленника и угроз АСУ ТП;
- большой раздел по типовым угрозам и уязвимостям АСУ ТП;

- рекомендации по созданию и реализации программы обеспечения безопасности АСУ ТП;
- подробное описание архитена сектуры АСУ ТП и общее описание подсистемы безопасности;
- всеобъемлющий раздел, посвященный всем классическим подсистемам информационной безопасности (контроль над доступом, идентификация и аутентификация, антивирусная защита, сети, аудиты, криптография и пр.) [8].

Необходимо подчеркнуть, что NIST SP 800-82 и Приказ ФСТЭК № 31 совершенно не противоречат друг другу. И хотя стандарт NIST является не единственным документом, который целесообразно использовать, он содержит все необходимые разделы и может применяться наряду с Приказом ФСТЭК № 31 при построении системы защиты автоматизированных систем управления. Также следует отметить, что в России стало распространенной практикой одновременное использование двух этих документов и, соответственно, подходов.

Литература

1. Гаврилов В. Фундамент безопасности АСУ ТП: от правовых основ до особых методик // М.: Connect. 2013. № 9.
2. Гарбук С.В., Комаров А.А., Салов Е.И. Аналитический отчет «Обзор инцидентов информационной безопасности АСУ ТП зарубежных государств» // М.: НТЦ «Станкинформзащита», 2010.
3. Кирилина Т.Ю. Использование современных информационных технологий при изучении социальной реальности. В сборнике: Современные образовательные технологии, используемые в очном, заочном и дополнительном образовании Сборник трудов по материалам Международной научно-практической Интернет-конференции. 2013. С. 151-159.
4. Кирилина Т.Ю., Кирилина Н.А. Российское и мировое доменное пространство: итоги и перспективы развития // Информационно-технологический вестник. 2017. Т. 12. № 2. С. 64-73.
5. Послание президента Федеральному собранию в 2016 году» [Электронный ресурс]. URL: https://ria.ru/politics/20161201/1482599559.html.
6. Приказ ФСТЭК № 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» // М: 2014г.
7. Указ Президента РФ от 5 декабря 2016 г. N 646 «Об утверждении Доктрины информационной безопасности Российской Федерации» [Электронный ресурс]. URL: http://www.garant.ru/hotlaw/federal/1036728/.
8. Guide to Industrial Control Systems (ICS) Security // U.S.: Special Publication 800-82, 2011 г.

9. Kaspersky Lab ICS CERT [Электронный ресурс]. URL: https://ics-cert.kaspersky.ru/.