www.volsu.ru

DOI: https://doi.org/10.15688/NBIT.jvolsu.2019.2.5

УДК 681.5
ББК 39.7

СРАВНЕНИЕ ТРЕБОВАНИЙ РЕГУЛЯТОРОВ РОССИЙСКОЙ ФЕДЕРАЦИИ И США К АВТОМАТИЧЕСКИМ СИСТЕМАМ УПРАВЛЕНИЯ ТЕХНОЛОГИЧЕСКИМИ ПРОЦЕССАМИ КРИТИЧЕСКИ ВАЖНЫХ ОБЪЕКТОВ

Вадим Юрьевич Шевцов

Ассистент кафедры информационной безопасности,
Волгоградский государственный университет
vadim94.d@mail.ru
просп. Университетский, 100, 400062 г. Волгоград, Российская Федерация

Евгений Сергеевич Абрамов

Кандидат технических наук, доцент,
заведующий кафедрой безопасности информационных технологий,
Южный федеральный университет
abramoves@sfedu.ru
ул. Б. Садовая, 105, 344006 г. Ростов-на-Дону, Российская Федерация

Аннотация. В статье приводится обзор законодательства в области АСУ ТП КВО в РФ и США. Приводится сравнение требований к данным системам регуляторов ФСТЭК и FIPS. Подробно рассматриваются следующие документы: приказ ФСТЭК России № 31 и FIPS 800-82 Rev 2.

Ключевые слова: АСУ ТП КВО, ICS, ФСТЭК, FIPS, информационная безопасность.

С каждым годом проблема кибербезопасности становится все более актуальной. Это происходит по ряду причин, основной из которых является повсеместное распространение информационных технологий. Данная проблема не обошла стороной автоматизированные системы управления технологическими процессами критически важных объектов (далее – АСУ ТП КВО), где безопасность стоит на первом месте. Если физическая безопасность критически важных объектов может быть решена на самом высоком уровне, то некоторые проблемы информационной безопасности (ИБ) вызывают ряд вопросов. Эти проблемы не являются уникальными для АСУ ТП КВО – они встречаются и в корпоративных сетях. Но несмотря на разную степень критичности, их распространенность в первом и втором случае несопоставима: в корпоративных сетях такие проблемы чаще бывают решены, в АСУ ТП КВО – гораздо реже из-за специфики данных сетей и заблуждений руководства [1].

В данной статье проводится сравнение нормативных правовых актов в области ин-

формационной безопасности АСУ ТП КВО РФ и США. В России к данным документам относятся:

– Федеральный закон от 26.07.2017 г. № 187-ФЗ «О безопасности критической информационной инфраструктуры Российской Федерации»;

– Федеральный закон от 26.07.2017 г. № 194-ФЗ «О внесении изменений в Уголовный кодекс Российской Федерации и статью 151 Уголовно-процессуального кодекса Российской Федерации в связи с принятием Федерального закона «О безопасности критической информационной инфраструктуры Российской Федерации»;

– Указ Президента РФ от 12.05.2009 г. № 537 «О Стратегии национальной безопасности Российской Федерации до 2020 года»;

– «Основы государственной политики в области обеспечения безопасности населения Российской Федерации и защищенности критически важных и потенциально опасных объектов от угроз природного, техногенного характера и террористических актов на период до 2020 года» (утв. Президентом РФ 15.11.2011 г., № Пр-3400);

– Распоряжение Правительства РФ от 27.08.2005 г. № 1314-р «Об одобрении Концепции федеральной системы мониторинга критически важных объектов и (или) потенциально опасных объектов инфраструктуры РФ и опасных грузов»;

– «Основные направления государственной политики в области обеспечения безопасности автоматизированных систем управления производственными и технологическими процессами критически важных объектов инфраструктуры Российской Федерации» (утв. Президентом РФ 03.02.2012 г., № 803);

– Концепция государственной системы обнаружения, предупреждения и ликвидации последствий компьютерных атак на информационные ресурсы Российской Федерации (утв. Президентом РФ 12.12.2014 г. № К 1274);

– «Методические рекомендации по формированию аналитического прогноза по укомплектованию подразделений по обеспечению безопасности информации в ключевых системах информационной инфраструктуры, противодействию иностранным техническим разведкам и технической защите информации подготовленными кадрами на заданный период» (утв. ФСТЭК России 23.04.2011 г.);

– Приказ ФСТЭК России № 31 от 14.03.2014 г. «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»;

– Информационное сообщение ФСТЭК России от 25.07.2014 г. № 240/22/2748 «По вопросам обеспечения безопасности информации в ключевых системах информационной инфраструктуры в связи с изданием приказа ФСТЭК России от 14 марта 2014 г. № 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»;

– ГОСТ Р 56205-2014 IEC/TS 62443-1-1:2009 Сети коммуникационные промышленные. Защищенность (кибербезопасность) сети и системы. Часть 1-1. Терминология, концептуальные положения и модели;

– ГОСТ Р МЭК 62443-2-1-2015 Сети коммуникационные промышленные. Защищенность (кибербезопасность) сети и системы. Часть 2-1. Составление программы обеспечения защищенности (кибербезопасности) системы управления и промышленной автоматики;

– ГОСТ Р 56498-2015 (IEC/PAS 62443-3:2008) Сети коммуникационные промышленные. Защищенность (кибербезопасность) сети и системы. Часть 3. Защищенность (кибербезопасность) промышленного процесса измерения и управления.

В США:

– Comprehensive National Cybersecurity Initiative;

– E-Government Act of 2002 including Title III – The Federal Information Security Management (FISMA) Act;

– International Strategy for Cyberspace;

– National Infrastructure Protection Plan;

– National Security Strategy;

– Presidential Policy Directive – Critical Infrastructure Security and Resilience;

– NIST SP 800-82 Rev 2, Guide to Industrial Control Systems (ICS) Security, May 2015;

– Rinaldi, et al, Identifying, Understanding, and Analyzing Critical Infrastructure Interdependencies, IEEE Control Systems Magazine, 2001;

– GAO-04-354, Critical Infrastructure Protection: Challenges and Efforts to Secure Control Systems, U.S. GAO, 2004;

– Stamp, Jason, et al., Common Vulnerabilities in Critical Infrastructure Control Systems, Sandia National Laboratories, 2003;

– Duggan, David, et al, Penetration Testing of Industrial Control Systems, Sandia National Laboratories, Report No SAND2005-2846P, 2005;

– ANSI/ISA-62443-3-3 (99.03.03)-2013 – Security for industrial automation and control systems Part 3-3: System security requirements and security levels.

Более подробно рассмотрим документы ФСТЭК и FIPS к требованиям по защите АСУ ТП КВО, так как их документы представляют основные требования к данным системам.

Главным документом ФСТЭК по требованиям к обеспечению защиты информации в АСУ ТП КВО является приказ от 14 марта 2014 г. № 31 «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». Он устанавливает требования к обеспечению защиты информации, обработка которой осуществляется автоматизированными системами управления производственными и технологическими процессами на критически важных объектах, потенциально опасных объектах, объектах, представляющих повышенную опасность для жизни и здоровья людей и для окружающей природной среды [2].

Аналогичный документ в FIPS – Special Publication 800-82 14.05.2013 «Guide to Industrial Control Systems (ICS) Security» [3]. Цель рекомендаций – обеспечить руководство для защиты АСУ ТП. Задачи рекомендаций – их типовое использование в объектах критически важной инфраструктуры. В отличие от приказа ФСТЭК № 31, данные рекомендации являются обязательными к исполнению в соответствующих государственных организациях. Также определяются исполнители (в документе ФСТЭК они определены более обобщенно):

– главные инженеры, интеграторы, архитекторы проектов, реализующих безопасность АСУ ТП;

– системные администраторы, инженеры и другие специалисты IT, кто администрирует, обновляет, защищает АСУ ТП;

– консультанты по безопасности, которые выполняют оценку безопасности и проникновения в АСУ ТП;

– руководство, которое оценивает риски и оправдывает применение средств и систем защиты;

– вендоры, занимающиеся внедрением продуктов, используемых в АСУ ТП.

В приказе ФСТЭК определяются уровни управления, компоненты, объекты защиты АСУ ТП. При этом нет описания реализаций данных определений. В этом плане SP 800-82 значительно превосходит приказ ФСТЭК № 31. Здесь описываются базовые операции в АСУ ТП на основе ключевых компонентов (контролируемая зона, терминалы управления, система удаленной диагностики и обслуживания) и компонентов сети предприятия (сеть компонентов АСУ ТП, сеть управления, маршрутизаторы, межсетевые экраны, модемы, точки удаленного доступа), есть обзор систем, применяемых АСУ ТП (SCADA, DCS и PLC), а также описываются основные особенности объектов АСУ ТП КВО США.

Обеспечение защиты для АСУ ТП в приказе ФСТЭК № 31 определяется следующими мероприятиями:

– формирование требований к защите информации в автоматизированной системе управления;

– разработка системы защиты автоматизированной системы управления;

– внедрение системы защиты автоматизированной системы управления и ввод ее в действие;

– обеспечение защиты информации в ходе эксплуатации автоматизированной системы управления;

– обеспечение защиты информации при выводе из эксплуатации автоматизированной системы управления.

Также определены меры защиты информации и их базовые наборы для соответствующего класса защищенности автоматизированной системы управления и ссылки на другие нормативно-правовые акты в дополнение к этому.

Рекомендации SP 800-82 включают целые разделы по следующим темам:

– характеристики, угрозы и уязвимости АСУ ТП (сравнение АСУ ТП и IT-систем, угрозы, потенциальные уязвимости, факторы риска, сценарии и источники инцидентов, документирование инцидентов);

– разработка и внедрение программ безопасности в АСУ ТП (бизнес-планирование ИБ, разработка комплексной программы безопасности);

– архитектура сети (межсетевые экраны, логическое разделение сети управления, разделение сетей, рекомендуемая архитектура многоэшелонной безопасности, политика межсетевых экранов, рекомендуемые правила межсетевых экранов для специальных сервисов, NAT, особые вопросы по межсетевым экранам, упавшие узлы, избыточность и отказоустойчивость, противодействие атакам типа Men in the Middle);

– контроль безопасности АСУ ТП (управленческий контроль, операционный контроль, технический контроль).

Дополнительно приводится список приложений, главные из которых: текущая деятельность в области безопасности систем промышленного контроля, новые возможности обеспечения безопасности, промышленные системы управления в парадигме FISMA.

На основе приведенного сравнительного анализа двух документов явно видно более высокое качество выполнения рекомендаций SP 800-82. В сравнении с ФСТЭК № 31 он имеет больший объем, описание защищаемых систем, конкретные рекомендации по жизненному циклу системы защиты АСУ ТП, особое внимание уделяется сетевому взаимодействию (все это не смотря на более позднюю разработку отечественного документа). Результаты сравнения мер защиты приведены в таблице

Таблица

Сравнение мер защиты рекомендаций SP 800-82 и приказа ФСТЭК № 31

Меры защиты	Приказ ФСТЭК от 14.03.14 № 31	800-82 Revision 2 Guide to ICS Security
1.	Идентификация и аутентификация (ИАФ) Identification and Authentication	
2.	Управление доступом субъектов доступа и объектов доступа (УПД)	Security Assessment and Authorization Access Control
3.	Ограничение программной среды (ОПС)	System and Information Integrity, Program Management
4.	Защита машинных носителей информации (ЗНИ)	Media Protection
5.	Аудит безопасности (АУД)	Audit and Accountability
6.	Антивирусная защита (АВЗ)	System and Information Integrity
7.	Предотвращение вторжений (СОВ)	System and Information Integrity
8.	Обеспечение целостности (ОЦЛ)	System and Information Integrity
9.	Обеспечение доступности (ОДТ) Access Control	
10.	Защита технических средств и систем (ЗТС) System and Services Acquisition	
11.	Защита информационной системы и ее компонентов (ЗИС) System and services acquisition	
12.	Реагирование на компьютерные инциденты (ИНЦ) Incident Response	
13.	Управление конфигурацией (УКФ) Configuration Management	
14.	Управление обновлениями программного обеспечения (ОПО) Maintenance	
15.	Планирование мероприятий по обеспечению безопасности (ПЛН)	Planning, Contingency Planning
16.	Информирование и обучение персонала (ДНС)	Awareness and Training, Personnel Security
17.		Physical and Environmental Protection
18.		System and Communications Protection
19.		Risk Assessment

(меры защиты в одной ячейке являются аналогичными).

В заключение следует добавить, что российским регуляторам ИБ следует использовать опыт иностранных коллег в области ИБ, ускорить создание новых стандартов и дополнение текущих, а также обязать АСУ ТП КВО к обязательному исполнению соответствующих требований к защите.

СПИСОК ЛИТЕРАТУРЫ

1. Информационная безопасность АСУ ТП КВО // Портал выбора технологий и поставщиков. – Электрон. текстовые дан. – Режим доступа: http://www.tadviser.ru/index.php/Статья:Информационная_безопасность_АСУ_ТП_КВО (дата обращения: 19.04.2019). – Загл. с экрана.

2. Об утверждении требований о защите информации, не составляющей государственную тайну, содержащейся в государственных информационных системах : Приказ ФСТЭК № 31 от 11 февраля 2014 г. – Доступ из информационных ресурсов ФСТЭК России.

3. National Institute of Standards and Technology. – Gaithersburg : NIST, 2015. – Guide to Industrial Control Systems (ICS) Security. – Доступ из информационных ресурсов FIPS.

REFERENCES

1. Informatsionnaya bezopasnost ASU TP KVO [Information Security of Automatic Process Control Systems for Critical Facilities]. *Portal vybora tekhnologiy i postavshchikov* [Portal for Choosing Technologies and Suppliers]. URL: http://www.tadviser.ru/index.php/Statya:Informacionnaya_bezopasnost_ASU_TP ekrana (accessed 19 April 2019).

2. Ob utverzhdenii trebovaniy o zashchite informatsii, ne sostavlyayushchey gosudarstvennuyu taynu, soderzhashcheysya v gosudarstvennykh informatsionnykh sistemakh : Prikaz FSTEK № 31 ot 11 fevralya 2014 g. [FSTEC Order no. 31 of February 11, 2014 "On Approving Requirements for the Protection of Information not Constituting a State Secret Contained in State Information Systems"]. *Dostup iz informatsionnykh resursov FSTEK Rossii* [Access from Information Resources of the Federal Service for Technical and Export Control].

3. National Institute of Standards and Technology. Gaithersburg: NIST, 2015. Guide to Industrial Control Systems (ICS) Security. *Access from Information Resources of the FIPS.*

COMPARISON OF REQUIREMENTS OF REGULATORS OF THE RUSSIAN FEDERATION AND THE UNITED STATES OF AMERICA TO AUTOMATIC CONTROL SYSTEMS OF TECHNOLOGICAL PROCESSES OF CRITICAL OBJECTS

Vadim Yu. Shevtsov

Assistant Lecturer, Department of Information Security,
Volgograd State University
vadim94.d@mail.ru
Prosp. Universitetsky, 100, 400062 Volgograd, Russian Federation

Evgeny S. Abramov

Candidate of Sciences (Engineering), Associate Professor,
Head of the Department of Information Technologies Security,
South Federal University
abramoves@sfedu.ru
St. B. Sadovaya, 105, 344006 Rostov-on-Don, Russian Federation

Abstract. There are requirements for AMS TP CO based on federal laws, the presidential decree, the FSTEC decree and documents, other information security conceptions, state

standards in the Russian Federation and requirements for ICS based on other security strategies, the FISMA Act, NIST, IEEE, GAO documents and others in the Unitet States of America.

The main FSTEC document for information security AMS TP CO is the decree of March 14, 2014 no. 31. The main FIPS document for information security ICS is Special Publication 800-82 Rev 2.

The FIPS document Special Publication 800-82 Rev 2 is more detailed than the FSTEC document in realization control levels, components, objects of ICS protection. The Special Publication includes base operations in ICS main components and enterprises network, ICS system review, USA critical object feature description.

Special Publication 800-82 Rev 2 shows more quality performance than the FSTEC document. It has more pages, system descriptions, recommendation for the life cycle security system of ICS, a lot of network contents.

Key words: AMS TP CO, ICS, FSTEC, FIPS, information security.