УДК 004.056.5 + 681.518 Вестник УрФО № 1(31) / 2019, с. 31–36

Баранкова И. И., Коновалов М. В., Пермякова О. В., Пермякова М. А.

DOI: 10.14529/secur190105

ПРОЕКТИРОВАНИЕ СИСТЕМЫ БЕЗОПАСНОСТИ АСУ ТП КАК ЗНАЧИМОГО ОБЪЕКТА КРИТИЧЕСКОЙ ИНФОРМАЦИОННОЙ ИНФРАСТРУКТУРЫ

В статье рассмотрены основные требования к созданию систем безопасности значимых объектов критической информационной инфраструктуры. Проведено исследование объекта на наличие уязвимостей, угроз безопасности информации, а также определены их источники. Составлена модель нарушителя информационной безопасности. Разработаны рекомендации к защите объекта, согласно нормативным требованиям, а также к защите верхнего и нижнего уровней АСУ ТП. Предложены варианты защиты периметра технологической сети. Сделан вывод о необходимости внедрения программного решения для предотвращения инцидентов информационной безопасности значимого объекта критической информационной инфраструктуры.

Ключевые слова: *критическая информационная инфраструктура, автоматизированная система управления технологическими процессами, система безопасности значимого объекта, угрозы безопасности информации, уязвимости программного обеспечения, модель нарушителя.*

Barankova I. I., Konovalov M. V., Permyakova O. V., Permyakova M. A.

SECURITY SYSTEM PROJECT DEVELOPMENT OF THE APCS AS A SIGNIFICANT OBJECT OF THE CRITICAL INFORMATION INFRASTRUCTURE

This paper covers the main requirements for the security system development of a significant object of the critical information infrastructure. The object is examined for vulnerabilities, information security threats and its sources are also determined. The adversary model is developed within the study. The recommendations for the object security system are given according to the normative concerns. The secure variants of the field network edge are proposed as the APCS levels protection. A conclusion about the relevancy of information security incident prevention software is drawn for the significant object of the critical information infrastructure.

Keywords: *critical information infrastructure, automated process control system, security system, information security threats, vulnerabilities, adversary model.*

В связи со вступлением в силу Федерального закона от 26.07.2017 № 187-ФЗ «О безопасности критической информационной инфраструктуры Российской Федерации» [1] и актуальностью проблемы защиты автоматизированных систем управления технологическими процессами (АСУ ТП), для снижения экономического ущерба предприятия в случае выхода систем из строя, возникает необходимость создания комплексной системы защиты информации (ЗИ) в АСУ ТП.

Объектами защиты в АСУ ТП являются:

– информация о параметрах управляемого объекта или процесса (входная/выходная информация, контрольно-измерительная информация, иная критически важная технологическая информация);

– программно-технический комплекс, включающий технические средства, программное обеспечение, а также средства ЗИ.

Система безопасности АСУ ТП как значимого объекта критической информационной инфраструктуры (ОКИИ) включает в себя правовые, организационные, технические и иные меры, направленные на обеспечение информационной безопасности субъектов КИИ [2], и обеспечивается за счет выполнения требований, утвержденных следующими нормативно-правовыми актами: приказом ФСТЭК от 14 марта 2014 г. № 31, приказом ФСТЭК от 25 декабря 2017 г. № 239, приказом ФСТЭК от 21 декабря 2017 г. № 235.

Требования направлены на обеспечение функционирования АСУ ТП в штатном режиме, при котором обеспечивается выполнение целевых функций АСУ ТП в условиях воздействия угроз безопасности информации (УБИ), а также на снижение рисков незаконного вмешательства в процессы функционирования АСУ ТП [3], и включают в себя:

– категорию значимости ОКИИ;

– определение УБИ, реализация которых может привести к нарушению штатного режима функционирования АСУ, и разработку модели УБИ;

– определение требований к системе защиты АСУ ТП.

Для внедрения организационных мер ЗИ в ОКИИ АСУ ТП необходимо:

1. ввести ограничения на действия персонала, а также на условия эксплуатации, изменение состава и конфигурации технических средств и программного обеспечения;

2. назначить администратора безопасности информации;

3. реализовать правила разграничения доступа субъектов доступа к соответствующим объектам;

4. провести проверку полноты и детальности описания в организационно-распорядительных документах по ЗИ действий персонала АСУ и администратора безопасности информации, направленных на обеспечение защиты информации;

5. отработать действия должностных лиц и подразделений, обеспечивающих эксплуатацию АСУ и ЗИ.

УБИ определяются на каждом из уровней АСУ ТП. Определение включает в себя: выявление источников УБИ и оценку потенциала нарушителей, анализ уязвимостей АСУ ТП, определение возможных сценариев реализации УБИ, оценку возможных последствий от реализации УБИ. В качестве исходных данных при определении УБИ используется банк данных угроз безопасности информации ФСТЭК.

Анализ уязвимостей объекта [4] включает четыре этапа (рисунок 1):

1. разработка модели действий нарушителей;

2. выявление и оценка основных видов угроз и возможного ущерба от их реализации;

3. оценка показателей уязвимости объекта и существующей системы безопасности, выделение особо важных зон и объектов и категорирование таких объектов;

4. оценка рисков потери ресурсов организации, на основании чего определяются пути нейтрализации угроз и формируются

общие рекомендации по обеспечению безопасности объекта.

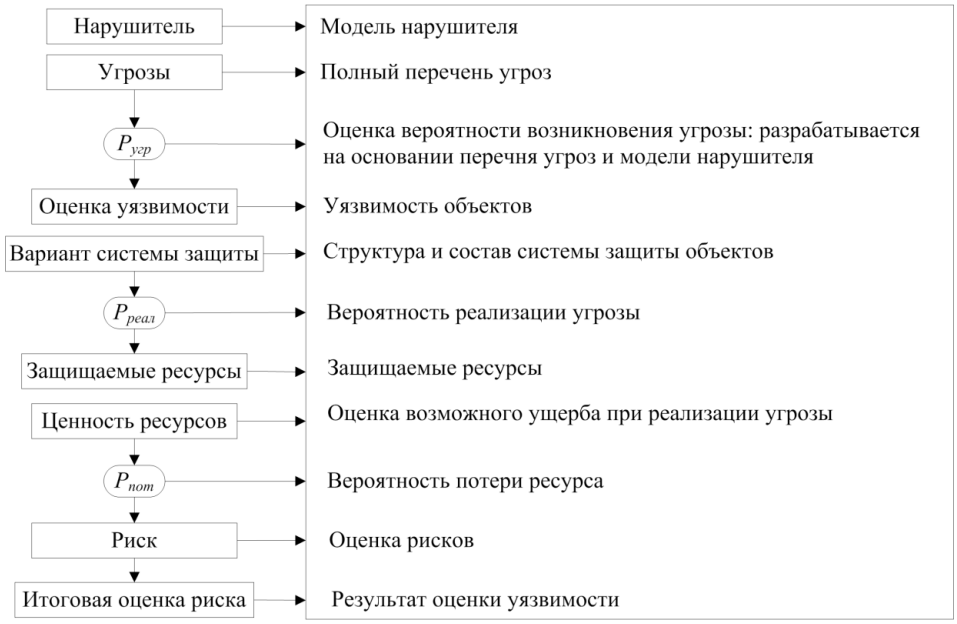

Рис. 1. Этапы оценки уязвимости объекта и рисков потери ресурсов

При выявлении источников УБИ составляется модель нарушителя, включающая в себя:

– категории нарушителей, которые могут воздействовать на объект;

– цели, которые могут преследовать нарушители каждой категории;

– типовые сценарии возможных действий нарушителей.

По наличию прав доступа нарушители подразделяются на два типа: внешние и внутренние. К внешним относятся: разведывательные службы государств, криминальные структуры, конкуренты, недобросовестные партнеры, внешние субъекты. Возможности внутреннего нарушителя зависят от действующих в пределах расположения АСУ ТП режимных и организационно-технических мер защиты, в том числе от допуска лиц и контроля порядка проведения работ.

Основными источниками угроз в АСУ ТП являются: вспомогательный персонал; инженерно-технический персонал; операторы АСУ ТП; разработчики компонентов АСУ ТП; количественная или качественная недостаточность компонентов АСУ ТП; внешний техногенный источник угроз. Модель нарушителя АСУ ТП представлена в таблице 1 (стр. 34).

Исследование потенциальных уязвимостей и УБИ проводилось на примере АСУ ТП установки электрического нагрева стали. В результате были выявлены следующие уязвимости программируемых логических контроллеров и специального программного обеспечения, связанные с: недостатками процедуры проверки пароля; повышением уровня привилегий злоумышленника; получением несанкционированного доступа к информации. Среди угроз безопасности АСУ ТП были выявлены:

– угрозы остановки объекта управления или отказа в обслуживании:

– возможность внедрения закладок в АСУ ТП (на уровне SCADA);

– угроза нарушения целостности системы, как на уровне программного обеспечения, так и на уровне оборудования (вирусы класса Stuxnet, заражающие программируемые логические контроллеры Siemens, Triton);

– угроза нарушения доступности из-за неправильного функционирования средств ЗИ;

– угроза несанкционированного доступа к АСУ ТП.

Создаваемая система безопасности значимого ОКИИ должна обеспечивать:

– предотвращение неправомерного доступа к информации;

– недопущение воздействия на технические средства обработки информации, в результате которого может быть нарушено или прекращено функционирование значимых объектов;

– восстановление функционирования значимых ОКИИ;

Таблица 1

Модель нарушителя в АСУ ТП

Категория нарушителя	Персонал АСУ ТП	Возможности нарушителя
первая	инженер-электроник, электрик	может изменять конфигурацию технических средств АСУ ТП, вносить в нее программно-аппаратные закладки; может располагать фрагментами информации о топологии АСУ ТП и об используемых коммуникационных протоколах и их сервисах; имеет возможность физического доступа к фрагментам локальной вычислительной сети (ЛВС) и аппаратным средствам АСУ ТП.
вторая	технологический персонал	знает не менее одного легального имени доступа; обладает всеми необходимыми атрибутами, обеспечивающими доступ к ресурсам АСУ ТП; может располагать информацией о топологии, технических средствах обработки информации и используемых коммуникационных протоколах и их сервисах; имеет возможность физического доступа к фрагментам ЛВС и аппаратным средствам АСУ ТП; обладает информацией об аппаратно-программных средствах и конфигурации АСУ ТП; обладает высоким уровнем знаний и опытом работы с техническими средствами АСУ ТП и их обслуживания.
третья	инженеры-программисты	обладает информацией об алгоритмах, программах и технологиях обработки информации в АСУ ТП; обладает возможностями внесения закладок в технические средства АСУ ТП на стадии их разработки, внедрения и сопровождения; может располагать любыми фрагментами информации о топологии АСУ ТП и технических средствах обработки и защиты информации в АСУ ТП

– непрерывное взаимодействие с ГосСОПКА, в соответствии со ст.5 Федерального закона №187-ФЗ.

В значимом ОКИИ не допускается:

– наличие удаленного доступа напрямую к программным/программно-аппаратным средствам, в том числе средствам ЗИ, для обновления или управления со стороны лиц, не являющихся работниками субъекта КИИ;

– наличие локального беспроводного доступа к программным/программно-аппаратным средствам, в том числе средствам ЗИ, для обновления или управления со стороны лиц, не являющихся работниками субъекта КИИ;

– передача информации, в том числе технологической информации, разработчику программных/программно-аппаратных средств, в том числе средств ЗИ, или иным лицам без контроля со стороны субъекта КИИ.

Для защиты серверов SCADA и АРМ-операторов должны использоваться сертифицированные промышленные средства антивирусной защиты, средства защиты от несанкционированного доступа, средства контроля действий привилегированных пользователей, средства контроля уровня защищенности.

Защита периметра технологической сети в АСУ ТП может быть реализована с помощью:

– сегментирования сети;

– реализации подсистемы межсетевого экранирования и подсистемы предотвращения вторжений на стыках технологических сетей, корпоративных и других не доверенных сетей;

– организации безопасного удаленного доступа с использованием сертифицированных алгоритмов шифрования (ГОСТ 28147-89, ГОСТ 34.12-2015);

– обеспечения защиты при передаче телемеханики сторонним организациям и контролирующим органам;

– организации однонаправленной передачи информации;

– анализа защищенности сети передачи данных.

Для предотвращения инцидентов на уровне контроллеров необходимо программное решение, отслеживающее состояние технологической сети; анализирующее трафик, передаваемый с использованием

промышленных протоколов, на предмет наличия аномальной активности, а также обнаруживающее сетевые атаки, запускаемые из внутренних источников.

Литература

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

2. Приказ ФСТЭК России от 21 декабря 2017 г. № 235 «Об утверждении Требований к созданию систем безопасности значимых объектов критической информационной инфраструктуры Российской Федерации и обеспечению их функционирования»

3. Приказ 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 здоровья людей и для окружающей природной среды»

4. Ворона В.А., Тихонов В.А., Митрякова Л.В. Теоретические основы обеспечения безопасности объектов информатизации. Учебное пособие для вузов. – М.: Горячая линия – Телеком, 2016. – 304 с.: ил.

References

1. Federal'nyy zakon ot 26.07.2017 № 187-FZ «O bezopasnosti kriticheskoy informatsionnoy infrastruktury Rossiyskoy Federatsii»

2. Prikaz FSTEK Rossii ot 21 dekabrya 2017 g. № 235 «Ob utverzhdenii Trebovaniy k sozdaniyu sistem bezopasnosti znachimykh ob"ektov kriticheskoy informatsionnoy infrastruktury Rossiyskoy Federatsii i obespecheniyu ikh funktsionirovaniya»

3. Prikaz FSTEK Rossii ot 14.03.2014 g. № 31 «Ob utverzhdenii trebovaniy k obespecheniyu zashchity informatsii v avtomatizirovannykh sistemakh upravleniya proizvodstvennymi i tekhnologicheskimi protsessami na kriticheski vazhnykh ob"ektakh, potentsial'no opasnykh ob"ektakh, a takzhe ob"ektakh, predstavlyayushchikh povyshennuyu opasnost' dlya zhizni zdorov'ya lyudey i dlya okruzhayushchey prirodnoy sredy»

4. Vorona V.A., Tikhonov V.A., Mitryakova L.V. Teoreticheskie osnovy obespecheniya bezopasnosti ob"ektov informatizatsii. Uchebnoe posobie dlya vuzov. – M.: Goryachaya liniya – Telekom, 2016. – 304 s.: il.

БАРАНКОВА Инна Ильинична, доктор технических наук, заведующий кафедрой Информатики и информационной безопасности Магнитогорского государственного технического университета им. Г. И. Носова. 455000, г. Магнитогорск, пр. Ленина, 38. E-mail: inna_barankova@mail.ru

КОНОВАЛОВ Максим Владимирович, кандидат технических наук, инженер-электроник СЦ ООО «ТЕХНОАП Инжиниринг» в г. Магнитогорск, г. Москва, Научный проезд, дом 20, строение 3. E-mail: mkovmgn@gmail.com

ПЕРМЯКОВА Ольга Валерьевна, старший преподаватель кафедры Информатики и информационной безопасности Магнитогорского государственного технического университета им. Г. И. Носова. 455000, г. Магнитогорск, пр. Ленина, 38. E-mail: mrs.permyakova.olga@gmail.com

ПЕРМЯКОВА Мария Александровна, студент кафедры Информатики и информационной безопасности Магнитогорского государственного технического университета им. Г. И. Носова. 455000, г. Магнитогорск, пр. Ленина, 38. E-mail: dear.irene.adler@gmail.com

BARANKOVA Inna, Department, Nosov Magnitogorsk State Technical University (NMSTU), D. Sc., Head of Computer Science and Information Safety Engineering (CSISE), Bld. 38, Lenina Ave, Magnitogorsk, Russia, 455000, E-mail: inna_barankova@mail.ru

KONOVALOV Maxim, SC LLC «TEHNOAP Engineering» in Magnitogorsk, Ph.D., electronics engineer, Moscow, Scientific passage, house 20, building 3. E-mail: mkovmgn@gmail.com

PERMYAKOVA Olga, NMSTU, Assistant Professor of CSISE Department, Bld. 38, Lenina Ave, Magnitogorsk, Russia, 455000, E-mail: mrs.permyakova.olga@gmail.com

PERMYAKOVA Maria, NMSTU, student, Bld. 38, Lenina Ave, Magnitogorsk, Russia, 455000, E-mail: dear.irene.adler@gmail.com