УДК 004.45 + 658.51-50 Вестник УрФО № 3(33) / 2019, с. 69–72

Зырянова Т. Ю., Медведев Н. В., Федорова Е. Н. DOI: 10.14529/secur190308

АНАЛИЗ ТРЕБОВАНИЙ ТРЕТЬЕЙ КАТЕГОРИИ ЗНАЧИМОСТИ ОБЪЕКТОВ КИИ В ИНФРАСТРУКТУРЕ ПРЕДПРИЯТИЯ

Федеральный закон Российской Федерации от 26.07.2017 № 187-ФЗ «О безопасности критической информационной инфраструктуры Российской Федерации» вступил в силу 1 января 2018 года. При этом, важным становится вопрос создания системы безопасности объектов критической информационной инфраструктуры.

Ключевые слова: *Критическая информационная инфраструктура, субъект КИИ, объект КИИ, категорирование объектов, АСУ ТП.*

Zyryanova T. Y., Medvedev N. V., Fedorova E. N.

ANALYSIS OF REQUIREMENTS OF THE THIRD CATEGORY OF SIGNIFICANCE OF CRITICAL INFORMATION INFRASTRUCTURE OBJECTS IN THE ENTERPRISE INFRASTRUCTURE

Federal Law of the Russian Federation dated July 26, 2017 No. 87 «About security of critical information infrastructure of the Russian Federation» entered into force on 1 January 2018. At the same time, the issue of creating a security system for critical information infrastructure facilities becomes important.

Keywords: *Critical information infrastructure, subject CII, object CII categorization of objects, SCADA.*

С развитием информационной сферы всё более актуальным является вопрос информационной безопасности автоматизированных систем управления технологическим процессом (далее – АСУ ТП), а также той инфраструктуры, которая её окружает. При этом использование систем безопасности АСУ ТП не должно нарушать её функционирование и снижать надежность системы. АСУ ТП многих предприятий могут рассматриваться как объект критической информационной

инфраструктуры (далее – КИИ), по отношению к которому необходимо проводить комплекс мероприятий по защите информации.

Критическая информационная инфраструктура – это объекты КИИ, а также сети электросвязи, используемые для организации взаимодействия таких объектов. К объектам КИИ относятся информационные системы, информационно-телекоммуникационные сети, автоматизированные системы управления субъектов КИИ[1]. В [2-3] представлены основные нормативно-правовые документы по обеспечению безопасности КИИ в РФ.

По статистике за 2018 год было зафиксировано более 4,3 млрд компьютерных атак на КИИ [4].

Цель нашего исследования – анализ и адаптация требований по обеспечению безопасности объектов КИИ, относящихся к 3 категории значимости с учетом использования типовой инфраструктуры технологического предприятия (сервера, АРМы, активное сетевое оборудование (далее – АСО), полевые устройства), а также определение минимального необходимого набора средств защиты информации (далее – СрЗИ).

Согласно требованиям к обеспечению безопасности в ходе создания, эксплуатации и вывода из эксплуатации значимых объектов, сначала необходимо установить требования к обеспечению безопасности значимого объекта, после чего разработать организационные и технические меры. Следующий этап заключается в реализации (внедрении) разработанных мер. После внедрения мероприятий необходимо обеспечить безопасность значимого объекта в ходе его эксплуатации и при выводе из эксплуатации.

Системы безопасности значимых объектов КИИ включают в себя организационно-распорядительные, технические и иные меры, направленные на обеспечение устойчивого функционирования значимых объектов при проведении в отношении них компьютерных атак. Организационные меры включают в себя создание регламентов, технические меры обеспечиваются встроенными средствами операционных систем (далее – ОС) и возможностями прикладного и специального программного обеспечения (далее – ПО).

К основным возможностям ОС, прикладного и специального ПО можно отнести идентификацию и проверку подлинности субъектов доступа при входе в систему по идентификатору и паролю, контроль доступа субъектов к защищаемым информационным ресурсам, контроль использования внешних носителей информации, регистрацию и учет входа (выхода) субъектов доступа в ОС и другие.

Технологическая инфраструктура предприятия обычно является многоуровневой, поэтому целесообразно рассматривать набор мер СрЗИ применительно к каждому уровню. Так в своей работе мы выделяем три основных уровня: сервера и АРМы, АСО, простые полевые устройства и датчики.

К примеру, для мер антивирусной защиты для серверов и АРМ – защита реализуется с помощью механизмов средства антивирусной защиты (далее САЗ), так как САЗ невозможно установить на простые полевые устройства, а только на АРМ или сервер. Как правило, большинство мер из базового набора не применимы для уровней АСО (управляемые, неуправляемые коммутаторы) и полевых устройств (датчики, контроллеры без ОС), так как отсутствует возможность установки дополнительных средств защиты на данные устройства, поэтому контроль и управление ими осуществляется на уровне серверов и АРМ.

Ниже представлена сводная таблица базовых мер для объектов КИИ третьей категории значимости с возможными способами реализации, адаптированными под предложенную классификацию уровней инфраструктуры предприятия.

Таким образом, для третьей категории значимости КИИ необходим следующий набор программно-аппаратных средств: межсетевые экраны, система сбора и анализа событий, средства антивирусной защиты технологического сегмента, система анализа защищенности, система резервного копирования.

Организационные меры включают в себя повышение компетенций персонала, разработку регламентов идентификации и аутентификации пользователей, парольной политики, управления доступом, учета, хранения и уничтожения информации, проведение внутреннего аудита безопасности, организации антивирусной защиты, обеспечения целостности информации, резервного копирования и восстановления информации, защиты технических средств и систем, реагирования на компьютерные инциденты, управления конфигурацией информационной системы, управления обновлениями, разработки мероприятий по обеспечению защиты информации, работы персонала, при возникновении угроз ИБ, работы в нештатных ситуациях.

Выбор средств реализации мер защиты является управленческим решением субъекта КИИ. При этом стоит отметить, что для технических мер большее предпочтение отдается встроенным средствам защиты информации. Установка и настройка данных средств может

Состав мер по обеспечению безопасности

Таблица 1

Меры	Инфраструктура предприятия		
	Сервера	АСО	Полевые устройства и датчики
ИАФ	Организационные меры: Разработка регламентов идентификации и аутентификации пользователей. Парольная политика.		
	Реализация подсистемы идентификации и аутентификации путем настройки встроенных возможностей ПО	Реализация подсистемы идентификации и аутентификации путем настройки встроенных возможностей АСО	Реализация подсистемы идентификации и аутентификации путем настройки встроенных возможностей ПЛК (далее программно-логический контролер)
УПД	Организационные мероприятия: Регламент управления доступом. Парольная политика.		
	Реализации подсистемы идентификации и аутентификации, путем настройки встроенных возможностей системного ПО	Реализации подсистемы идентификации и аутентификации, путем настройки встроенных возможностей АСО	Реализации подсистемы идентификации и аутентификации, путем настройки встроенных возможностей ПЛК
ЗНИ	Организационные мероприятия: Регламент по учету, хранению и уничтожению информации.		
	Реализуется с использованием встроенных возможностей ОС, системного ПО и с использованием механизмов защиты средства антивирусной защиты	-	-
АУД	Организационные мероприятия: Регламент проведения внутреннего аудита безопасности.		
	Реализуется с использованием механизмов защиты средства анализа защищенности, системы сбора и анализа событий и средства антивирусной защиты	Реализуется с использованием встроенных возможностей АСО	Реализуется с использованием встроенных возможностей прикладного ПО
АВЗ	Организационные мероприятия: Регламент организации антивирусной защиты		
	Реализуется с использованием механизмов защиты средства антивирусной защиты	-	-
ОЦЛ	Организационные мероприятия: Регламент обеспечения целостности информации.		
	Реализуется встроенными функциями контроля целостности ПО		
ОДТ	Организационные мероприятия: Регламент резервного копирования и восстановления информации		
	Реализуется с использованием механизмов защиты системы резервного копирования		
ЗТС	Организационные мероприятия: Регламент защиты технических средств и систем		
ЗИС	Организационные мероприятия		
	Реализуется с использованием механизмов защиты межсетевого экрана и сегментирования сети	-	-
ИНЦ	Организационные мероприятия: Регламент реагирования на компьютерные инциденты		
	Реализуется с использованием механизмов защиты системы анализа защищенности и системы сбора и анализа событий	-	-
УКФ	Организационные мероприятия: Регламент управления конфигурацией ИС		
	Реализуется с использованием механизмов защиты системы сбора и анализа событий	Реализуется с использованием встроенных возможностей АСО	-
ОПО	Организационные мероприятия: Регламент управления обновлениями ПО		
	Реализуется с использованием механизмов защиты системы сбора и анализа событий	-	-
ПЛН	Организационные мероприятия: Регламент разработки мероприятий по обеспечению защиты информации. Приказ о назначении ответственных за обеспечение контроля выполнения мероприятий по защите информации		
ДНС	Организационные мероприятия: Регламент работы персонала, при возникновении угроз ИБ.		
	Реализуется с использованием механизмов защиты система резервного копирования	-	
ИПО	Организационные мероприятия: Регламент работы персонала, при возникновении угрозы ИБ. Регламент работы в нештатных ситуациях.		

осуществляться как самим субъектом КИИ, так и с привлечением подрядной организации, имеющей лицензию на осуществление деятельности в области технической защиты информации.

Литература

1. О безопасности критической информационной инфраструктуры Российской Федерации: федер. закон Рос. Федерации от 26 июля 2017 г. № 187-ФЗ: принят Гос. Думой 12 июля 2017 г.: одобр. Советом Федерации 19 июля 2017 г. // СПС Консультант Плюс

2. Об утверждении требований по обеспечению безопасности значимых объектов критической информационной инфраструктуры Российской Федерации: приказ ФСТЭК России 25 декабря 2017 г. N 239 (в ред. Приказа ФСТЭК России от 26 марта 2019 Г. N 60) // СПС Консультант Плюс

3. Об утверждении требований к созданию систем безопасности значимых объектов критической информационной инфраструктуры Российской Федерации и обеспечения их функционирования: Приказ ФСТЭК России от 21 декабря 2017 г. N 235 // СПС Консультант Плюс

4. Иван Егоров. Более 4 млрд кибератак на РФ зафиксировали специалисты в 2018 году [Электронный ресурс]: Российская газета, электронная версия [2018]. URL: https://rg.ru/2018/12/11/bolee-4-mlrd-kiberatak-na-rf-zafiksirovali-specialisty-v-2018-godu.html/

References

1. O bezopasnosti kriticheskoy informatsionnoy infrastruktury Rossiyskoy Federatsii: feder. zakon Ros. Federatsii ot 26 iyulya 2017 g. № 187-FZ: prinyat Gos. Dumoy 12 iyulya 2017 g.: odobr. Sovetom Federatsii 19 iyulya 2017 g. // SPS Konsul'tant Plyus

2. Ob utverzhdenii trebovaniy po obespecheniyu bezopasnosti znachimykh ob"yektov kriticheskoy informatsionnoy infrastruktury Rossiyskoy Federatsii: prikaz FSTEK Rossii 25 dekabrya 2017 g. N 239 // SPS Konsul'tant Plyus

3. Ob utverzhdenii trebovaniy k sozdaniyu sistem bezopasnosti znachimykh ob"yektov kriticheskoy informatsionnoy infrastruktury Rossiyskoy Federatsii i obespecheniya ikh funktsionirovaniya: Prikaz FSTEK Rossii ot 21 dekabrya 2017 g. N 235 // SPS Konsul'tant Plyus

4. Ivan Yegorov. Boleye 4 mlrd kiberatak na RF zafiksirovali spetsialisty v 2018 godu [Elektronnyy resurs]: Rossiyskaya gazeta, elektronnaya versiya [2018]. URL: https://rg.ru/2018/12/11/bolee-4-mlrd-kiberatak-na-rf-zafiksirovali-specialisty-v-2018-godu.html/

ЗЫРЯНОВА Татьяна Юрьевна, заведующий кафедрой «Информационные технологии и защита информации» Уральского государственного университета путей сообщения, канд. тех. наук. 620034, г. Екатеринбург, ул. Колмогорова, д. 66. E-mail: tzyryanova@usurt.ru

ZYRYANOVA Tatiana, associate professor of Department «Information Technology and Information Security» of the Ural State University of Railway Transport. Bld. 66, Kolmogorova str., Yekaterinburg, 620034. E-mail: tzyryanova@usurt.ru

МЕДВЕДЕВ Никита Владимирович, доцент кафедры «Информационные технологии и защита информации» Уральского государственного университета путей сообщения, канд. тех. наук. 620034, г. Екатеринбург, ул. Колмогорова, д. 66. E-mail: nmedvedev@usurt.ru

MEDVEDEV Nikita, associate professor of Department «Information Technology and Information Security» of the Ural State University of Railway Transport. Bld. 66, Kolmogorova str., Yekaterinburg, 620034. E-mail: nmedvedev@usurt.ru

ФЕДОРОВА Екатерина Николаевна, студентка 2 курса электротехнического факультета по направлению подготовки Информационная безопасность Уральского государственного университета путей сообщения, 620034 Екатеринбург, ул. Колмогорова, 66. E-mail: catherina.n-fedorova@yandex.ru

FEDOROVA Ekaterina, 2-year student of Department «Information Technology and Information Security» of the Ural State University of Railway Transport. Bld. 66, Kolmogorova str., Yekaterinburg, 620034. E-mail: catherina.n-fedorova@yandex.ru