УДК 004.056.5 + 003.26 Вестник УрФО № 4(30) / 2018, с. 66–74

Васильев В. И. , Кириллова А. Д. , Кухарев С. Н.

DOI: 10.14529/secur180410

КИБЕРБЕЗОПАСНОСТЬ АВТОМАТИЗИРОВАННЫХ СИСТЕМ УПРАВЛЕНИЯ ПРОМЫШЛЕННЫХ ОБЪЕКТОВ (СОВРЕМЕННОЕ СОСТОЯНИЕ, ТЕНДЕНЦИИ)[1]

Последние годы характеризуются резким ростом актуальности проблемы обеспечения кибербезопасности автоматизированных систем управления технологическими процессами (АСУ ТП) промышленных объектов. В данной статье рассматривается общее состояние данной проблемы и пути ее решения. Основное внимание уделяется анализу существующей нормативно-методической и правовой базы обеспечения кибербезопасности критически важных объектов. Дается краткая характеристика основных положений ключевых документов в области кибербезопасности АСУ ТП (NIST SP 800-82, NERC CIP, ISA/IEC 62443, Федеральный закон № 187-ФЗ, Приказы ФСТЭК Рос-сии №№ 31 и 239, ГОСТ Р МЭК 62443).Отмечается активная роль указанных документов в решении практических задач, связанных с обеспечением кибербезопасности.

Ключевые слова: *кибербезопасность, автоматизированная система управления, технологический процесс, стандарт, оценка риска.*

Vasilyev V. I. , Kirillova A. D. , Kukharev S. N.

CYBERSECURITY OF APCS: MODERN TRENDS AND APPROACHES (CURRENT STATE, PERSPECTIVES)

Last years are characterized by sharp increase of urgency of the problem connected with providing the cybersecurity of automated process control systems (APCS) of industrial objects. The given paper investigates a general state of this problem and the ways of its solving. The main attention is paid to analysis of existing normative-methodical and legal base of cybersecurity maintenance of critically important objects. The brief characteristic of main principles

[1] Исследование выполнено при финансовой поддержке РФФИ в рамках научного проекта № 17-48-020095

containing in some key documents in APCS cybersecurity sphere (NIST SP 800-82, NERC CIP, ISA/IEC 62443, Federal Law 187-FZ, FSTEC of Russia Orders No. 31 and 239, GOST R 62443 series) is given. The active role of these documents in solving practical tasks connected with providing cybersecurity is emphasized.

Keywords: *cybersecurity, automated process control systems, technological process, standard, risk assessment.*

Введение

Статистика последних лет подтверждает резкий рост числа хакерских атак на автоматизированные системы управления технологическими процессами (АСУ ТП) крупных и средних промышленных предприятий. Так, по материалам исследований «Лаборатории Касперского» [1] только во втором полугодии 2017 г. около половины (46,8%) компьютеров, используемых в системах промышленной автоматизации в России, хотя бы один раз подвергались компьютерным атакам. В 2017 г. 10,8% всех систем АСУ ТП стали мишенью атак ботнет-агентов. Основными источниками атак ботнет-агентов при этом были Интернет, сменные носители и сообщения электронной почты. В качестве наиболее крупных целевых атак на системы промышленной инфраструктуры в 2017 г. наибольшую известность получили вирус-шифровальщик WannaCry (на него пришлось 13,4% от всех атакованных компьютерных систем технологической инфраструктуры организаций), а также широко нашумевшие атаки Industroyer и Trisis/Triton. Особенностью 2-х последних атак является то, что впервые после вируса Stuxnet атакующим удалось создать собственные реализации промышленных сетевых протоколов и получить возможность напрямую влиять на работу управляющих устройств в составе АСУ ТП.

Общее число уязвимостей, выявленных в различных компонентах АСУ ТП экспертами «Лаборатории Касперского» в 2017 г., составило 322. Наибольшее количество уязвимостей было выявлено в:

– компонентах SCADA-систем (т.е. систем диспетчерского управления и сбора данных);

– сетевых устройствах промышленного назначения;

– программируемых логических контроллерах (ПЛК);

– инженерном программном обеспечении (ПО).

Как отмечается в [1], эксплуатация злоумышленниками указанных уязвимостей может привести к выполнению произвольного кода, несанкционированному управлению промышленным оборудованием, отказу в его работе. При этом значительная часть уязвимостей может эксплуатироваться удаленно без аутентификации, и их эксплуатация не требует от злоумышленника каких-либо специальных знаний и навыков.

Приведенные факты являются безусловным доказательством обострения ситуации, складывающейся вокруг обеспечения безопасности систем промышленной автоматизации. Это особенно касается потенциально опасных производств и объектов критической инфраструктуры в области энергетики, нефтехимии, водоснабжения, транспорта и т.п., реализация атак на которые может привести к серьезным последствиям для жизни и здоровья людей или нанесению ущерба окружающей среде. Сегодня фактически уже общепризнано, что безопасность АСУ ТП не сводится к обеспечению информационной безопасности (ИБ), т.е. обеспечению конфиденциальности собираемой, обрабатываемой и передаваемой информации. Безопасность АСУ ТП должна заключаться прежде всего в обеспечении непрерывности и целостности самого ТП, что составляет содержание нового, бурно развивающегося направления «кибербезопасность» (cybersecurity) АСУ ТП [2-4].

Вместе с тем, хотя на Западе термины «киберпространство», «кибербезопасность» уже давно заняли свое прочное место в профессиональной среде, в России все еще продолжаются споры относительно сути самого понятия «кибербезопасность» и сферы его применения [5-7]. На данный момент в российском законодательстве понятие «киберпространство» и «кибербезопасность» отсутствуют. Вынесенная в начале 2014 г. на обсуждение «Концепция стратегии кибербезопасности Российской Федерации» [8] получила неоднозначные оценки и так и не была принята. В то же время, сегодня наметилось определенное противоречие между отставанием нормативно-правовой базы и многочисленными предложениями на рынке в области обеспечения кибербезопасности АСУ ТП со стороны веду-

щих российских компаний («ДиалогНаука», «ИнфоТеКС», «Лаборатория Касперского», «Информзащита», Positive Technologies, «Ростелеком» и др.). В июле 2018 г. в Москве состоялся Международный конгресс по кибербезопасности, одной из главных целей которого явилась координация усилий и планов совместных действий производителей и специалистов в сфере кибербезопасности.

Учитывая актуальность затронутой проблемы, рассмотрим современное состояние нормативно-правового и методического обеспечения работ в области кибербезопасности АСУ ТП. Для определенности далее будем пользоваться следующим определением кибербезопасности, приведенном на сайте Cisco [9]: **кибербезопасность** – это реализация мер по защите систем, сетей и программных приложений от цифровых атак.

Американские и международные стандарты в области кибербезопасности АСУ ТП

Наиболее известными стандартами, имеющими непосредственное отношение к проблеме кибербезопасности АСУ ТП, являются следующие стандарты, изначально разработанные в США и получившие широкое распространение по всему миру:

1) NIST SP 800-82 «Guide to Industrial Control Systems (ICS) Security»;

2) NERC Critical Infrastructure Protection (CIP), Cybersecurity;

3) ANSI/ISA-99 «ISA-99 Security for Industrial Automation and Control Systems»;

4) ISA/IEC 62443 «Industrial Automation and Control Systems Security».

Стандарт NIST SP 800-82 («Рекомендации по обеспечению безопасности промышленных систем автоматизации») разработан Центром компьютерной безопасности (CSRC) Национального института стандартов и технологий (NIST, National Institute of Standards and Technology) в 2011 г. (2-ая редакция – в 2015 г.).

Данный стандарт фактически представляет собой набор практических рекомендаций и методических наработок по комплексному обеспечению безопасности АСУ ТП [10]. Стандарт NIST содержит:

– рекомендации, связанные с построением системы защиты информации;

– упрощенные модели злоумышленника и угроз АСУ ТП;

– перечень типовых угроз и уязвимостей АСУ ТП;

– рекомендации по созданию и внедрению программы обеспечения безопасности АСУ ТП;

– описание архитектуры типовой АСУ ТП и подсистемы безопасности;

– описание традиционных подсистем ИБ (контроля и управления доступом, идентификации и аутентификации, антивирусной защиты и др.).

Семейство отраслевых стандартов NERC-CIP (Critical Infrastructure Protection) – «Защита объектов критической инфраструктуры» – разработаны Северо-Американской корпорацией по обеспечению надежности электросетей (NERC, North American Electric Reliability Corporation) в начале 2000-х гг. Целью применения данных стандартов является обеспечение надежной защиты автоматизированных систем и сетей коммуникации для объектов энергетического сектора от возможных кибератак [10]. В состав данного семейства стандартов входят стандарты NERC CIP-001÷009, в том числе:

– CIP-002-1 Critical Cyber Asset Identification («Идентификация критических киберактивов);

– CIP-005-1 Electronic Security Perimeter («Электронный периметр безопасности»);

– CIP-006-1 Physical Security («Физическая безопасность»);

– CIP-007-1 Systems Security Management («Управление безопасностью систем»).

Как и стандарт NIST SP 800-82, стандарты NERC CIP представляют собой детально проработанные методические руководства по обеспечению кибербезопасности АСУ ТП (в данном случае – объектов в энергетической сфере), которые успешно применяются не только в США, но и во многих странах мира, включая Россию.

Семейство стандартов ANSI/ISA-99 («Безопасность промышленных систем автоматизации и управления») – это комплексная программа обеспечения безопасности АСУ ТП, разработанная комитетом ISA-99 в составе Международного общества автоматизации (ISA, International Society of Automation), отвечающим за разработку стандартов. В 2007 г. стандарт ISA-99 был поддержан Американским национальным институтом стандартов (ANSI, American National Institute of Standards) и был опубликован как ANSI/ISA-99, а в 2010 г. переиздан как ANSI/ISA-62443 [11].

В качестве базовой концепции в этих

стандартах используется подход, основанный на сегментации сети передачи данных предприятия на зоны и связывающие их тракты (пути сообщения). Под зоной при этом понимается объединение логических или физических средств, для которых предъявляются схожие требования по безопасности, например, критичность для ТП. В стандартах не определены конкретные методы или алгоритмы выделения зон и трактов внутри сети передачи данных. Вместо этого предлагается осуществлять такой выбор (с обоснованием соответствующих требований к ним по обеспечению безопасности) исходя из анализа уровня рисков компании. Риск в данном случае заключается не столько в самой возможности реализации кибератаки, сколько в ее последствиях, а уменьшение последствий достигается за счет локализации их в выделенной зоне, максимально изолированной от других сегментов. Обеспечение безопасности зон и каналов осуществляется путем выбора специализированных средств защиты, например, промышленных межсетевых экранов или VPN.

Предложенная в указанных стандартах концепция обеспечения безопасности АСУ ТП на основе сегментации (зонирования) системы получила поддержку Международной электротехнической комиссии (IEC, International Electrotechnical Commission) и в дальнейшем легла в основу разработки стандартов кибербезопасности АСУ ТП нового поколения ISA/IEC 62443.

Серия международных стандартов ISA/IEC 62443 («Безопасность промышленных систем автоматизации и управления») – это совместная перспективная разработка комитетов ISA-99 и IEC, имеющая своей целью обеспечение безопасности, доступности, целостности и конфиденциальности компонентов и систем, входящих в состав промышленных АСУ ТП [13].

Работа над созданием стандартов ведется начиная с 2009 г. Всего предполагается выпуск 13 ключевых стандартов и технических отчетов, разделенных на 4 группы:

1) «Общие положения» (General) – 2 стандарта и 2 технических отчета, определяющие базовые понятия, модели, термины, количественные показатели (метрики) безопасности АСУ ТП;

2) «Политики и процедуры» (Policies and Procedures) – 2 стандарта и 2 технических отчета, устанавливающие общие требования к системе управления защитой АСУ ТП, а также ряд конкретных правил в рамках программы безопасности АСУ ТП;

3) «Системные требования» (System Requirements) – 1 стандарт и 2 технических отчета, описывающие различные технологии обеспечения безопасности АСУ ТП, оценки рисков и контроля уровня защищенности системы;

4) «Требования к компонентам» (Component Requirements) – 2 стандарта, определяющие требования к безопасности на уровне отдельных подсистем и компонентов АСУ ТП (нижний уровень).

В настоящее время часть этих стандартов уже опубликована, другие находятся в процессе разработки и утверждения.

В основе требований, предъявляемых стандартами ISA/IEC 62443 к обеспечению безопасности АСУ ТП, лежит риск-ориентированный подход. В соответствии с этим подходом, проектирование системы управления защитой АСУ ТП предполагает выполнение следующих этапов:

– высокоуровневая (ориентировочная) оценка рисков от воздействия кибератак;

– построение *референсной (reference)* модели АСУ ТП как объекта защиты, описывающей классификацию основных видов деятельности, ТП, АСУ и других активов;

– построение *модели активов* (asset model), описывающей иерархию основных объектов и активов АСУ ТП, их взаимодействие с сетями, ключевыми подразделениями и т.д.;

– построение *референсной модели архитектуры* (reference architecture model), отражающей все основные элементы АСУ ТП, телекоммуникационное оборудование, линии связи и т.п.;

– построение *модели зонирования* (zone and conduit model), разделяющей объект защиты на отдельные зоны;

– детальный *анализ рисков* для каждой выделенной зоны;

– определение *текущего уровня безопасности* для каждой зоны и требований по обеспечению *целевого уровня безопасности* зоны, реализуемых путем выбора соответствующих мер защиты.

Ряд стандартов серии ISA/IEC 62443 сегодня переведены на русский язык и активно используются ведущими российскими компаниями – лидерами рынка систем защиты АСУ ТП.

Нормативно-правовые основы обеспечения кибербезопасности АСУ ТП в России

Одним из базовых нормативно-законодательных актов, определяющих общие требования к безопасности промышленных объектов, является **федеральный закон «О безопасности объектов топливно-энергетического комплекса» от 21 июля 1997 г. № 116-ФЗ** (последняя редакция с изменениями 2018 г.). Этот закон устанавливает организационные и правовые основы в сфере обеспечения безопасности объектов топливно-энергетического комплекса (ТЭК). В соответствии со статьей 11 этого закона, определена необходимость создания на объектах ТЭК системы защиты информации и информационно-телекоммуникационных сетей от неправомерного доступа, уничтожения, модифицирования, блокирования информации и иных неправомерных действий.

Конкретные требования, предъявляемые к системам защиты АСУ ТП промышленных предприятий, определены **Приказом 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 среды» [14]. В рамках Приказа рассматривается 3-хуровневая структура АСУ ТП, включающая в себя: уровень ввода-вывода данных (датчики, исполнительные механизмы), уровень автоматического управления (программируемые логические контроллеры, ПЛК) и уровень операторского управления (АРМ, SCADA-серверы, телекоммуникационное оборудование).

В качестве объектов защиты АСУ ТП выделяются:

– критически важная (технологическая) информация, включающая управляющую, контрольно-измерительную информацию и др.;

– программно-технический комплекс, включающий технические средства, ПО и средства защиты информации.

Требования к защите АСУ ТП определяются в зависимости от *класса защищенности* системы, который, в свою очередь, зависит от *уровня значимости (критичности)* обрабатываемой информации. Уровень значимости (критичности) информации определяется степенью возможного ущерба от нарушения ее целостности, доступности или конфиденциальности, в результате которого возможно нарушение штатного режима функционирования АСУ или незаконное вмешательство в процессы функционирования АСУ ТП.

Для каждого класса защищенности в Приказе ФСТЭК № 31 определены базовые наборы мер защиты, в состав которых входят:

1) идентификация и аутентификация;
2) управление доступом;
3) ограничение программной среды;
4) защита машинных носителей информации;
5) регистрация событий безопасности;
6) антивирусная защита;
7) обнаружение вторжений;
8) контроль (анализ) защиты информации;
9) обеспечение целостности;
10) обеспечение доступности;
11) защита среды виртуализации и др.

Выбранные меры защиты рассматриваются отдельно для каждого уровня АСУ ТП с учетом особенностей функционирования каждого из уровней.

Достоинством предложенного в Приказе ФСТЭК № 31 подхода к обеспечению защиты информации, обрабатываемой в АСУ ТП, является комплексное применение организационных и технических мер защиты информации на всех стадиях жизненного цикла АСУ ТП. В то же время, следует заметить, что требования Приказа, хотя и в значительной степени коррелируют с перечисленными выше международными стандартами, также носят рекомендательный (не обязательный) характер. Окончательное решение о выборе класса защищенности и необходимых мер защиты принимает собственник АСУ ТП.

Важную роль в решении проблемы безопасности АСУ ТП крупных промышленных предприятий играет **федеральный закон «О безопасности критической информационной инфраструктуры Российской Федерации» от 26 июля 2017 г. № 187-ФЗ** [15]. Под объектами критической информационной инфраструктуры (КИИ) здесь понимаются информационные системы, информационно-телекоммуникационные сети, автоматизированные системы управления субъектов РФ, функционирование которых критически важно для экономики государства. В соответствии с данным законом, должно производиться категорирование объектов КИИ, составляется общегосударственный реестр

значимых объектов КИИ, предусмотрено выполнение обязательных требований по обеспечению безопасности значимых объектов КИИ, контролируемых государством.

С целью конкретизации требований, предусмотренных федеральным законом 187-ФЗ, и условий их применения, ФСТЭК России выпустила **Приказ «Об утверждении Требований по обеспечению безопасности значимых объектов критической информационной инфраструктуры Российской Федерации» от 25 декабря 2017 г. № 239** [16]. В этом документе даются рекомендации по обеспечению безопасности значимых объектов на различных стадиях (этапах) их жизненного цикла:

а) установление требований к обеспечению безопасности значимого объекта;

б) разработка организационных и технических мер по обеспечению безопасности значимого объекта;

в) внедрение организационных и технических мер по обеспечению безопасности значимого объекта и ввода его в действие;

г) обеспечение безопасности значимого объекта в ходе его эксплуатации;

д) обеспечение безопасности значимого объекта при выводе его из эксплуатации.

Перечислен состав базового набора мер по обеспечению безопасности для значимых объектов КИИ различных категорий значимости.

Серия стандартов ГОСТ Р МЭК 62443 «Сети коммуникационные промышленные. Защищенность (кибербезопасность) сети и системы» – издается в России начиная с 2015 г. в рамках политики гармонизации системы национальных стандартов и приведения ее в соответствие с международной системой стандартов в области обеспечения безопасности АСУ ТП. Последнее очень важно для унификации терминологии, понятийной базы и формирования согласованных подходов и взаимодополняющих технических решений в условиях резкого обострения проблемы кибер-безопасности АСУ ТП, проявляющегося в форме глобального нарастания интенсивности кибератак и тяжести их последствий.

В настоящее время в России переведены и приняты следующие стандарты серии 62443:

– ГОСТ Р 56205-2014 IEC/TS 62443-1-1:2009 «Терминология, концептуальные положения и модели» (введен 01.01.2016);

– ГОСТ Р МЭК 62443-2-1-2015 (IEC 62443-2) «Составление программы обеспечения защищенности (кибербезопасности) системы управления и промышленной автоматики» (введен 01.01.2016);

– ГОСТ Р 56498 IEC 62443-3-3-2016 «Требования к системной безопасности и уровни безопасности» (введен 01.04.2017).

Ожидается продолжение выпуска данной серии по мере завершения работы над запланированными версиями стандартов ISA/IEC 62443. Очевидно, что в данном случае специалисты и организации, занимающиеся задачами проектирования, эксплуатации и аудита комплексных систем обеспечения безопасности АСУ ТП, получат в свое распоряжение мощный инструментарий для достижения поставленных перед ними целей. Вместе с тем, необходимо отметить, что «узким местом» указанных выше нормативных документов, регламентирующих вопросы обеспечения кибербезопасности АСУ ТП, является отсутствие формализованных методик детальной оценки рисков кибербезопасности. Как отмечается в ГОСТ Р 56205-2014 IEC/TS 62443-1-1, в настоящее время можно считать более или менее отработанными лишь методики ориентировочной (качественной) оценки рисков, применяемые для качественного сравнения уровней безопасности АСУ ТП. По мере увеличения объема статистических данных и разработки математических моделей риска, угроз и инцидентов безопасности, актуальной становится задача разработки методов и алгоритмов количественной оценки риска, обеспечивающих возможность обоснованного выбора устройств АСУ ТП и необходимых контрмер как в пределах отдельных зон безопасности, так и при обеспечении требуемого уровня кибербезопасности АСУ ТП в целом.

В качестве перспективного способа решения данной задачи можно указать активно ведущиеся в последние годы исследования, связанные с получением количественной оценки рисков (ущерба) на основе технологий интеллектуального анализа данных. Подобные исследования включают в себя такие направления, как:

а) разработку моделей и алгоритмов оценки рисков с использованием нечеткой логики и нейронных сетей [17-19];

б) разработку моделей и алгоритмов оценки рисков с использованием технологий когнитивного моделирования [20, 21];

в) разработку моделей и алгоритмов оценки рисков с использованием динамических байесовских сетей и скрытых марковских моделей [22, 23].

Заключение

Статистика последних лет показывает, что проблема обеспечения защищенности (кибербезопасности) АСУ ТП в условиях резкого нарастания числа и интенсивности кибератак, а также масштабов их последствий становится все более актуальной. Отсюда понятен интерес к разработке национальных и международных стандартов в области защиты АСУ ТП, устанавливающих требования к комплексным системам обеспечения безопасности критически важных объектов и рекомендации по выбору и реализации соответствующих мер защиты. Среди наиболее известных нормативных документов в области кибербезопасности АСУ ТП выделяют стандарты NIST SP 800-82, NERC CIP, ANSI/ISA-99, IEC 62443, а в нашей стране – Федеральный закон № 187-ФЗ, Приказы ФСТЭК России №№ 31 и 239, стандарты ГОСТ Р МЭК 62443. Отличительной чертой указанных документов является использование системного риск-ориентированного подхода к решению задач обеспечения безопасности АСУ ТП на всех этапах жизненного цикла. Особую роль при этом должно сыграть применение технологий интеллектуального анализа данных, позволяющих дать более точную количественную оценку рисков кибербезопасности и, как следствие, обеспечить более обоснованный выбор устройств АСУ ТП и необходимых контрмер для реализации стратегии многоуровневой эшелонированной защиты (defense in depth).

Литература

1. Ландшафт угроз для систем промышленной автоматизации, второе полугодие 2017 [Электронный ресурс]. URL: https://ics-cert.kaspersky.ru/reports/2018/03/26/threat-landscape-for-industrial-automation-systems-in-h2-2017 (дата обращения 26.07.2018).

2. Корольков С., Ярушевский Д. Обеспечение безопасности автоматизированных систем управления технологическими процессами/Пресс-Центр «ДиалогНаука» [Электронный ресурс]. URL: https://www.dialognauka.ru/press-center/article/141148 (дата обращения 26.07.2018).

3. Ярушевский Д. Кибербезопасность АСУ ТП – что это и зачем? [Электронный ресурс]. URL: https://www.dialognauka.ru/press-center/article/13226 (дата обращения 26.07.2018).

4. Массель Л. В., Воропай Н. И., Сендеров С. М., Массель А. Г. Кибербезопасность как одна из стратегических угроз энергетической безопасности России // Вопросы кибербезопасности. 2016. № 4 (17). С. 2–10.

5. Безкоровайный М. М., Татузов А. Л. Кибербезопасность – подходы к определению понятия // Вопросы кибербезопасности. 2014. № 1 (2). – С. 22–27.

6. Алпеев А. С. Терминология безопасности: кибербезопасность, информационная безопасность // Вопросы кибер-безопасности. 2014. № 5 (8). – С. 39–42.

7. Ватрушкин А. А. Правовые основы обеспечения кибер-безопасности критической инфраструктуры Российской Федерации // Евразийская адвокатура. 2017. № 6 (31).– С. 78–84.

8. Концепция стратегии кибербезопасности Российской Федерации (проект) [Электронный ресурс]. URL: http://www.council.gov.ru/media/files/41d4b3dfbd b25cea8a 73.pdf (дата обращения 26.07.2018).

9. Что такое кибербезопасность? [Электронный ресурс]. URL: https://www.cisco.com/c/ru_ru/products/security/what-is-cybersecurity.html (дата обращения 26.07.2018).

10. Обзор стандарта безопасности промышленных систем управления NIST SP 800-82 Rev. 2 [Электронный ресурс]. URL: https://www.ussc.ru/news/id/254 (дата обращения 26.07.2018).

11. Лукацкий А. Применимость стандартов NERC CIP в России / Безопасность инфраструктуры энергоснабжения [Электронный ресурс]. URL: http://www.rza-expo.ru/images/2017/history/2013/day4/C.5-7.pdf (дата обращения 26.07.2018).

12. Байрс Э. Использование стандартов ANSI/ISA-99 для обеспечения безопасности системы управления промышленным предприятием // Современные технологии автоматизации. 2014. № 1. – С. 6–15.

13. Ярушевский Д. Обеспечение безопасности АСУ ТП – краткий обзор семейства стандартов IEC 62443 // Information Security/Информационная безопасность. 2014. № 3 [Электронный ресурс]. URL: http://www.itsec.ru/articles2/Oborandteh/obespechenie-bezopasnosti-asu-tp-kratkiy-obzor-semeystva-standartov-iec-62443 (дата обращения 26.07.2018).

14. 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 окружающей среды / Приказ ФСТЭК России от 14 марта 2014 г. № 31 [Электронный ресурс]. URL: https://fstec.ru/normotvorcheskaya/akty/53-prikazy/868-prikaz-fstek-rossii-ot (дата обращения 26.07.2018).

15. Федеральный закон № 187-ФЗ «О безопасности критической информационной инфраструктуры Российской Федерации» от 26.07.2017 [Электронный ресурс]. URL: https://www.consultant.ru/document/cons_doc_LAW_220885/ (дата обращения 26.07.2018).

16. Об утверждении Требований по обеспечению безопасности значимых объектов критической информационной инфраструктуры Российской Федерации / Приказ ФСТЭК России от 25 декабря 2017 г. № 239 [Электронный ресурс]. URL: https://fstec.ru/normotvorcheskaya/akty/53-prikazy/868-prikaz-fstek-rossii-ot (дата обращения 26.07.2018).

17. Глушенко С. А., Долженко А. И. Система поддержки принятия решений нечеткого моделирования рисков информационной безопасности организации // Информационные технологии, Т. 21, № 1, 2015. – С. 68-74.

18. Булдакова Т. И., Миков Д. А. Методика анализа информационных рисков с применением нейро-нечеткой сети // НТИ. Сер. 2. Информационные процессы и системы, № 4, 2015. – С. 13-17.

19. Кириллова А. Д., Васильев В. И. Применение нечеткой нейронной сети для оценки рисков информационной безопасности АСУ ТП // Проблемы информационной безопасности / Материалы VII Всеросс. Заочной Интернет-конференции, 20-21 февр. 2018 г. – Ростов-на-Дону: Изд-во ООО «Азов Принт», 2018. – С. 138-142.

20. Васильев В. И., Вульфин А. М., Кудрявцева Р. Т. Анализ и управление рисками информационной безопасности с использованием технологий когнитивного моделирования // Доклады ТУСУР, Т. 20, № 4, г. Томск, 2017. – С. 61-66.

21. Васильев В. И., Вульфин А. М., Гузаиров М. Б., Кириллова А. Д. Интервальное оценивание информационных рисков с помощью нечетких серых когнитивных карт // Информационные технологии, Т. 24, № 10, 2018. – С. 657-664.

22. Арустамов С. А., Дайнеко В. Ю. Применение динамической байесовской сети в системах обнаружения вторжений // Научно-технический вестник информационных технологий, механики и оптики, № 3 (79), 2012. – С. 128-133.

23. Козачек А. В. Математическая модель системы распознавания разрушающих программных средств на основе скрытых марковских моделей // Вестник СибГУТИ, № 3, 2012. – С. 29-39.

References

1. Landshaft ugroz dlya sistem promyshlennoy avtomatizatsii, vtoroye polugodiye 2017 [Elektronnyy resurs]. URL: https://ics-cert.kaspersky.ru/reports/2018/03/26/threat-landscape-for-industrial-automation-systems-in-h2-2017 (data obrashcheniya 26.07.2018).

2. Korol'kov S., Yarushevskiy D. Obespecheniye bezopasnosti avtomatizirovannykh sistem upravleniya tekhnologicheskimi protsessami/Press-Tsentr «DialogNauka» [Elektronnyy resurs]. URL: https://www.dialognauka.ru/press-center/article/141148 (data obrashcheniya 26.07.2018).

3. Yarushevskiy D. Kiberbezopasnost' ASU TP – chto eto i zachem? [Elektronnyy resurs]. URL: https://www.dialognauka.ru/press-center/article/13226 (data obrashcheniya 26.07.2018).

4. Massel' L. V., Voropay N. I., Senderov S. M., Massel' A. G. Kiberbezopasnost' kak odna iz strategicheskikh ugroz energeticheskoy bezopasnosti Rossii // Voprosy kiberbezopasnosti. 2016. № 4 (17). – S. 2–10.

5. Bezkorovaynyy M. M., Tatuzov A. L. Kiberbezopasnost' – podkhody k opredeleniyu ponyatiya // Voprosy kiberbezopasnosti. 2014. № 1 (2). – S. 22–27.

6. Alpeyev A. S. Terminologiya bezopasnosti: kiberbezopasnost', informatsionnaya bezopasnost' // Voprosy kiber-bezopasnosti. 2014. № 5 (8). – S. 39–42.

7. Vatrushkin A. A. Pravovyye osnovy obespecheniya kiber-bezopasnosti kriticheskoy infrastruktury Rossiyskoy Federatsii // Yevraziyskaya advokatura. 2017. № 6 (31). – S. 78–84.

8. Kontseptsiya strategii kiberbezopasnosti Rossiyskoy Federatsii (proyekt) [Elektronnyy resurs]. URL: http://www.council.gov.ru/media/files/41d4b3dfbd b25cea8a 73.pdf (data obrashcheniya 26.07.2018).

9. Chto takoye kiberbezopasnost'? [Elektronnyy resurs]. URL: https://www.cisco.com/c/ru_ru/products/security/what-is-cybersecurity.html (data obrashcheniya 26.07.2018).

10. Obzor standarta bezopasnosti promyshlennykh sistem upravleniya NIST SP 800-82 Rev. 2 [Elektronnyy resurs]. URL: https://www.ussc.ru/news/id/254 (data obrashcheniya 26.07.2018). 11. Lukatskiy A. Primenimost' standartov NERC CIP v Rossii / Bezopasnost' infrastruktury energosnabzheniya [Elektronnyy resurs]. URL: http://www.rza-expo.ru/images/2017/history/2013/day4/C.5-7.pdf (data obrashcheniya 26.07.2018).

12. Bayrs E. Ispol'zovaniye standartov ANSI/ISA-99 dlya obespecheniya bezopasnosti sistemy upravleniya promyshlennym predpriyatiyem // Sovremennyye tekhnologii avtomatizatsii. 2014. № 1. – S. 6–15.

13. Yarushevskiy D. Obespecheniye bezopasnosti ASU TP – kratkiy obzor semeystva standartov IEC 62443 // Information Security/Informatsionnaya bezopasnost'. 2014. № 3 [Elektronnyy resurs]. URL: http://www.itsec.ru/articles2/Oborandteh/obespechenie-bezopasnosti-asu-tp-kratkiy-obzor-semeystva-standartov-iec-62443 (data obrashcheniya 26.07.2018).

14. Ob utverzhdenii trebovaniy k obespecheniyu zashchity informatsii v avtomatizirovannykh sistemakh upravleniya proizvodstvennymi i tekhnologicheskimi protsessami na kriticheski vazhnykh ob"yektakh, potentsial'no opasnykh ob"yektakh, a takzhe ob"yektakh, predstavlyayushchikh povyshennuyu opasnost' dlya zhizni i zdorov'ya lyudey i okruzhayushchey sredy / Prikaz FSTEK Rossii ot 14 marta 2014 g. № 31 [Elektronnyy resurs]. URL: https://fstec.ru/normotvorcheskaya/akty/53-prikazy/868-prikaz-fstek-rossii-ot (data obrashcheniya 26.07.2018).

15. Federal'nyy zakon № 187-FZ «O bezopasnosti kriticheskoy informatsionnoy infrastruktury Rossiyskoy Federatsii» ot 26.07.2017 [Elektronnyy resurs]. URL: https://www.consultant.ru/document/cons_doc_LAW_220885/ (data obrashcheniya 26.07.2018).

16. Ob utverzhdenii Trebovaniy po obespecheniyu bezopasnosti znachimykh ob"yektov kriticheskoy informatsionnoy infrastruktury Rossiyskoy Federatsii / Prikaz FSTEK Rossii ot 25 dekabrya 2017 g. № 239 [Elektronnyy resurs]. URL: https://fstec.ru/normotvorcheskaya/akty/53-prikazy/868-prikaz-fstek-rossii-ot (data obrashcheniya 26.07.2018).

17. Glushenko S. A., Dolzhenko A. I. Sistema podderzhki prinyatiya resheniy nechetkogo modelirovaniya riskov informatsionnoy bezopasnosti organizatsii // Informatsionnyye tekhnologii, T. 21, № 1, 2015. – S. 68-74.

18. Buldakova T. I., Mikov D. A. Metodika analiza informatsionnykh riskov s primeneniyem neyro-nechetkoy seti // NTI. Ser. 2. Informatsionnyye protsessy i sistemy, № 4, 2015. – S. 13-17.

19. Kirillova A. D., Vasil'yev V. I. Primeneniye nechetkoy neyronnoy seti dlya otsenki riskov informatsionnoy bezopasnosti ASU TP // Problemy informatsionnoy bezopasnosti / Materialy VII Vseross. Zaochnoy Internet-konferentsii, 20-21 fevr. 2018 g. – Rostov-na-Donu: Izd-vo OOO «Azov Print», 2018. – S. 138-142.

20. Vasil'yev V. I., Vul'fin A. M., Kudryavtseva R. T. Analiz i upravleniye riskami informatsionnoy bezopasnosti s ispol'zovaniyem tekhnologiy kognitivnogo modelirovaniya // Doklady TUSUR, T. 20, № 4, g. Tomsk, 2017. – S. 61-66.

21. Vasil'yev V. I., Vul'fin A. M., Guzairov M. B., Kirillova A. D. Interval'noye otsenivaniye informatsionnykh riskov s pomoshch'yu nechetkikh serykh kognitivnykh kart // Informatsionnyye tekhnologii, T. 24, № 10, 2018. – S. 657-664.

22. Arustamov S. A., Dayneko V. YU. Primeneniye dinamicheskoy bayyesovskoy seti v sistemakh obnaruzheniya vtorzheniy // Nauchno-tekhnicheskiy vestnik informatsionnykh tekhnologiy, mekhaniki i optiki, № 3 (79), 2012. – S. 128-133.

23. Kozachek A. V. Matematicheskaya model' sistemy raspoznavaniya razrushayushchikh programmnykh sredstv na osnove skrytykh markovskikh modeley // Vestnik SibGUTI, № 3, 2012. – S. 29-39.

ВАСИЛЬЕВ Владимир Иванович, доктор технических наук, профессор кафедры «Вычислительная техника и защита информации» ФГБОУ ВО «Уфимский государственный авиационный технический университет», Россия, 450008, г. Уфа, ул. К.Маркса, 12. E-mail: vasilyev@ugatu.ac.ru.

КИРИЛЛОВА Анастасия Дмитриевна, магистр, программист кафедры «Вычислительная техника и защита информации» ФГБОУ ВО «Уфимский государственный авиационный технический университет», Россия, 450008, г. Уфа, ул. К.Маркса, 12. E-mail: kirillova.andm@gmail.com

КУХАРЕВ Сергей Николаевич, аспирант кафедры «Вычислительная техника и защита информации» ФГБОУ ВО «Уфимский государственный авиационный технический университет», Россия, 450008, г. Уфа, ул. К.Маркса, 12. E-mail: kuharev.sn@zaorczi.ru

VASILYEV Vladimir, Dr. Sc. (Eng.), Professor of the Department «Computer Engineering and Information Security» FGBOU VO «Ufa State Aviation Technical University», 12 K.Marx Str., Ufa 450008, Russia. E-mail: vasilyev@ugatu.ac.ru.

KIRILLOVA Anastasiya, M. Sc., programmer of the Department «Computer Engineering and Information Security» FGBOU VO «Ufa State Aviation Technical University», 12 K.Marx Str., Ufa 450008, Russia. E-mail: kirillova.andm@gmail.com

KUKHAREV Sergey, post-graduate of the Department «Computer Engineering and Information Security» FGBOU VO «Ufa State Aviation Technical University», 12 K.Marx Str., Ufa 450008, Russia. E-mail: kuharev.sn@zaorczi.ru