УДК 004.056

А.Н. Каменских, Д.А. Бортник

Пермский национальный исследовательский политехнический университет, г. Пермь, Россия

АНАЛИЗ РЕКОМЕНДАЦИЙ ПО ЗАЩИТЕ АВТОМАТИЗИРОВАННЫХ СИСТЕМ УПРАВЛЕНИЯ С ЦЕЛЬЮ ВЫЯВЛЕНИЯ ТИПИЧНЫХ УЯЗВИМОСТЕЙ

Автоматизированная система управления технологическим процессом (АСУ ТП) – группа решений технических и программных средств, предназначенных для автоматизации управления технологическим оборудованием на промышленных предприятиях. Современные АСУ ТП непосредственно управляют сложными и опасными технологическими процессами. Аварии по причине уязвимости АСУ ТП в таких отраслях, как электроэнергетика, химическая, нефтегазовая и транспортная, могут привести к огромному ущербу не только в бизнесе, но и к тяжелым экологическим последствиям, в том числе и для здоровья и жизни людей. Риск техногенных катастроф определяется не только надежностью системы, но и ее безопасностью. В статье рассматриваются основные уязвимости АСУ ТП на основе анализа документа NISTSP 800-82. Уязвимость – это любая характеристика или свойство информационной системы, использование которой нарушителем может привести к реализации угрозы. Производя атаку, нарушитель использует какую-либо уязвимость системы, т.е. для надежной защиты системы, в данном случае АСУ ТП, следует найти и устранить как можно больше критических уязвимостей. В статье приводится классификация типичных и наиболее опасных уязвимостей на причины их возникновения, а также рекомендации по устранению данных уязвимостей на основе анализа архитектуры АСУ ТП, а также этапов ее жизненного цикла. Рассматриваются разные аспекты проектирования и функционирования автоматизированной системы управления: разработка системы, настройка, обслуживание, сетевые соединения и другие. Каждому аспекту присущи свои уязвимости. Их анализ позволяет соотнести требования и рекомендации российских стандартов с международным опытом.

Ключевые слова: АСУ ТП, информационная безопасность, уязвимость, SP 800-82.

A.N. Kamenskih, D.A. Bortnik

Perm National Research Polytechnic University, Perm, Russian Federation

ANALYSIS OF GUIDE TO ICS SECURITY TO IDENTIFY THE TYPICAL VULNERABILITIES

ICS it is a group of solutions of hardware and software designed to automate the control of technological equipment at industrial organizations. Modern ICSs directly manage complex and dangerous processes, a failure in which can lead to accidents at work and man-made disasters. In this article the main vulnerability of automation systems based on document NIST SP 800-82 is considered. Vulnerability is some characteristic or property of an information system, the use of which by the offender can lead to the realization of the threat. Attacking the system, the offender uses some vulnerability. For

reliable protection of the system, in this case, ICS, we have to find and fix all vulnerabilities. The article provides a classification of generic vulnerabilities, their causes, as well as recommendations to eliminate these vulnerabilities. This classification use two basic attribute – the content and architecture of ICS and life cycle. We consider the different aspects of the design and operation of an industrial control system: system engineering, configuration, maintenance, network connections and others. Each aspect can have its own vulnerabilities. The analysis of vulnerabilities allows comparing Russian guides for ICS security with world experience in ICS security incidents.

Keywords: ICS, information security, vulnerability, SP 800-82.

Введение. В настоящее время уделяется большое внимание вопросам безопасности, автоматизированных систем управления (АСУ). Причиной этого стал ряд успешных атак на АСУ ТП, приведших к серьезным последствиям. Одной из таких атак был Stuxnet, который является одним из самых известных червей. Впервые он был обнаружен в Иране. Червь поразил около трети центрифуг на заводе по обогащению урана в Натанзе, а также сорвал сроки запуска АЭС в Бушере. Ущерб, нанесенный ядерным объектам Ирана, сопоставим с ущербом от атаки израильских ВВС [1]. «Живя» в системе, червь накапливает информацию о режимах работы оборудования и в какой-то момент меняет их. Если, например, завысить установку по температуре, то агрегат будет продолжать работать после перегрева до полного самоуничтожения. При этом на экране АРМ оператор продолжает видеть нормальные значения и установки, которые червь подменяет в реальном времени. Еще одна интересная особенность вируса – искать активное интернет-соединение и отправлять информацию на определенные адреса. Также червь умеет обновлять себя через Интернет, и именно этим обусловлен тот факт, что у разных аналитиков выловленные копии вируса сильно отличаются [2]. Последствия атак на критические объекты (КО) [3], которые, как правило, оборудованы системами АСУ, могут нанести огромный ущерб, в том числе привести к гибели людей. В то же время большинство руководящих документов ФСТЭК по защите КО носят гриф «для служебного пользования» [4], что существенно затрудняет широкое обсуждение проблемы профессиональным сообществом. Поэтому при анализе авторы ориентировались на комплекс документов NIST по безопасности АСУ и АСУ ТП [5, 6].

Одним из базовых факторов безопасности АСУ ТП является их существенное отличие от обычных систем поддержки бизнеса, это обусловливает необходимость либо связывать их в единую систему в составе КСЗИ [7], либо создавать обособленное подразделение, специализирующееся на защите АСУ ТП [8].

Для надежной защиты АСУ ТП необходимо знать уязвимости, характерные именно для АСУ ТП, чтобы затем разработать эффективные меры по защите АСУ ТП и реализовать их в составе комплексной системы защиты информации предприятия.

1. Классификация уязвимостей. SP 800-82 – комплексное руководство по безопасности АСУ ТП, представляющее читателю рекомендации, обеспечивающие полный цикл разработки системы защиты АСУ ТП от постановки задачи до реализации и эксплуатации. Согласно руководству уязвимости в АСУ ТП можно классифицировать следующим образом:

– уязвимости в политике безопасности мероприятий по ее реализации;
– уязвимости в разработке и архитектуре системы;
– уязвимости в настройке и обслуживании;
– физические уязвимости;
– уязвимости в разработке программного обеспечения;
– уязвимости в коммуникации и настройке сети.

Сеть АСУ ТП, как показано на рисунке, состоит из многих взаимосвязанных компонентов.

Для обеспечения устойчивой работы АСУ ТП невозможно отказаться от этих компонентов, которые повышают ее безопасность. Таким образом, появляется множество уязвимостей, что, в свою очередь, требует адекватных мер по защите. Уязвимости могут возникнуть на любом участке архитектуры АСУ ТП. Следует учитывать, что сеть АСУ ТП может быть соединена с внешней сетью (например, Интернетом) для организации обслуживания и возможности оказать управляющее воздействие в случае экстренной ситуации. Классификация уязвимостей в NISTSP 800-82 адресована ключевым компонентам и этапам жизненного цикла АСУ ТП, в дальнейшем будет показано, почему важно учитывать обе эти составляющие.

2. Уязвимости в политике безопасности мероприятий по ее реализации. Политика безопасности – совокупность документированных правил, направленных на обеспечение безопасности предприятия. Очень часто бывает, что политика безопасности не доработана или является неподходящей для данной системы. Это приводит к наличию уязвимостей в АСУ. Каждая мера противодействия должна быть отражена в политике, это обеспечивает единообразие и отчетность.

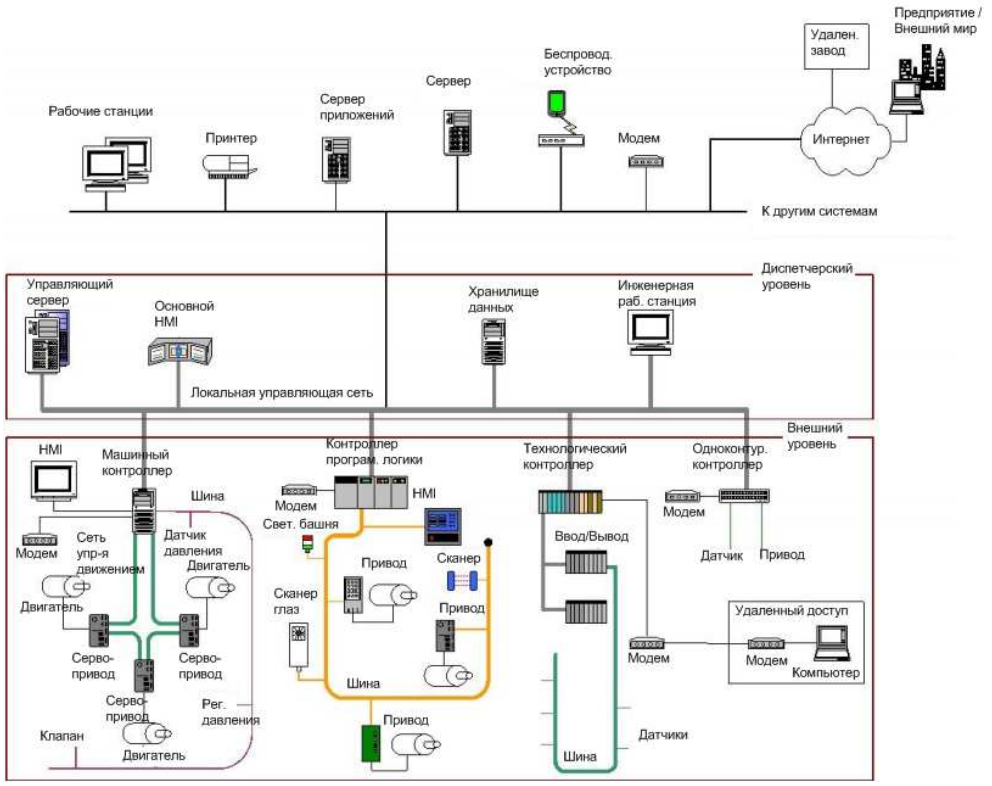

Рис. Структура сети АСУ

Чтобы быть эффективной, политика безопасности должна включать в себя политику управления конфигурацией АСУ, управления доступом и аутентификации, а также учитывать мобильные и переносные устройства, используемые с АСУ.

Необходимо держать персонал в курсе политики безопасности и мероприятий по ее реализации, а также в курсе угроз, стандартов информационной безопасности и рекомендаций по защите.

Чтобы убедиться, что политика и ее составные элементы управления реализованы правильно, работают и производят желаемый эффект в отношении безопасности АСУ, должны проводиться аудит и оценка рисков.

Одной грамотно разработанной политики мало, необходимо, чтобы на предприятии действовали организационные меры по ее соблюдению. Персонал, не следующий политике, должен подвергаться различным видам исправительных воздействий. Политика должна быть ясной в отношении последствий несогласия с ней.

Если в системе все-таки произошел взлом, система должна каким-то образом на это отреагировать. Это позволит уменьшить потери и быстрее восстановить нормальное функционирование АСУ.

Также должен быть разработан план действий при нештатных ситуациях, таких как сбои оборудования или разрушение здания. Отсутствие такого плана может обернуться большим временем простоя и потерей продукции.

Уязвимости этой группы в основном связаны с действиями персонала, а также с недостаточным пониманием особенностей АСУ, SCADA или РСУ. Таким образом, необходимо при разработке системы безопасности (СБ) руководствоваться специально разработанными под АСУ рекомендациями, требованиями и стандартами, простое копирование стандартов для других систем приведет к появлению большого числа уязвимостей.

3. Уязвимости в разработке и архитектуре системы. Система может разрабатываться без учета возможных угроз и уязвимостей. Затем, по мере необходимости, компоненты защиты включаются в структуру. Такой подход является опасным.

Система защиты должна включаться в архитектуру АСУ еще на стадии разработки. Структура системы защиты является частью структуры предприятия. Система защиты должна включать в себя аутентификацию и авторизацию пользователей, механизмы управления доступом, топологию сети, системные настройки и механизмы обеспечения целостности. Если у АСУ нет четко определенных границ контролируемой зоны, то нельзя гарантировать, что механизмы защиты функционируют правильно. Это может стать причиной несанкционированного доступа к системе и данным, а также других проблем.

Такие сервисы, как DNS и DHCP, использующиеся защищенными сетями, часто реализуются в обычных сетях. В результате этого сеть АСУ становится зависимой от обычной сети, в которой не выполняются принципы доступности и целостности, необходимые для АСУ.

Может случиться так, что без точного и надлежащего протоколирования не удастся выявить причину взлома. Взлом может произойти незаметно, что приведет к дополнительным повреждениям и/или нарушениям. Для выявления проблем с механизмами защиты, такими как неправильная настройка и сбои, необходим регулярный мониторинг безопасности.

В отличие от классических СБ при защите АСУ свойства доступности и целостности имеют гораздо большее значение, чем конфиденциальность. В связи с этим встраивать СБ в АСУ необходимо еще на этапе проектирования АСУ.

4. Уязвимости в настройке и обслуживании. Помимо вопросов создания политики безопасности и разработки системы внимание стоит уделять также настройке и обслуживанию этой системы.

В любой момент времени должно быть известно, какое оборудование, прошивки и программное обеспечение используются АСУ. Если на предприятии не реализован процесс для учета вышеперечисленного, это может привести к установке небезопасных настроек и появлению дыр в защите. Для надежной защиты должен быть точный список активов и текущих настроек.

Чтобы не поставить под угрозу нормальное функционирование АСУ, любые изменения в системе должны проходить длительные комплексные тестирования. Для критически важных настроек необходима возможность восстановления после случайного или преднамеренного воздействия на систему.

В используемой ОС и программном обеспечении могут быть обнаружены новые уязвимости. Чтобы не поставить под угрозу безопасность АСУ, должны быть разработаны документированные процедуры по поддержке обновлений.

Если конфиденциальные данные (например, пароли, телефонные номера) хранятся в открытом виде на переносных устройствах (ноутбуках, мобильных телефонах) и эти устройства утеряны, то система защиты может быть взломана.

Для защиты от вредоносного ПО должны быть установлены и настроены антивирусные средства защиты. Антивирусные базы должны всегда обновляться, так как в условиях очень динамично развивающейся среды устаревшие антивирусы могут сделать систему открытой для новых вредоносных программ.

Помимо вредоносного ПО система может быть подвержена DoS-атакам, в результате которых могут возникнуть задержки в работе системы. Взломы могут привести к нарушению целостности и доступности системы; получению, изменению и потере данных; неправильному выполнению управляющих команд. Системы обнаружения и предотвращения вторжений могут остановить или предотвратить

различные виды атак, включая DoS-атаки, а также определить атакованные компьютеры, например, зараженные червями.

Уязвимости этой группы достаточно типичны для всех больших вычислительных систем, однако компоненты АСУ зачастую работают под загрузкой, близкой к 100 %, кроме того, они могут быть распределены территориально на многие десятки километров, если речь идет о нефтепроводах. Таким образом, задача администрирования безопасности АСУ значительно усложняется, и происходит увеличение уровня угрозы для этих уязвимостей.

5. Физические уязвимости. Физическое воздействие на систему также может привести к серьезным последствиям. Чтобы их предотвратить, физический доступ к оборудованию АСУ должен быть разрешен только для уполномоченного персонала. Неправомерный доступ к оборудованию АСУ может привести:

– к физической краже данных и оборудования;

– физическому повреждению или уничтожению данных и оборудования;

– отключению физических каналов передачи данных;

– несанкционированным изменениям в функциональной части (например, несанкционированное использование сменных носителей, добавление/удаление ресурсов);

– незамеченному перехвату данных (нажатие клавиш и другие события ввода).

Кроме того, незащищенные USB- и PS/2-порты могут стать причиной несанкционированного подключения флэш-накопителей, кейлоггеров и т.п.

Оборудование, используемое для управления системой, уязвимо для радиочастотных и электромагнитных импульсов. Это воздействие может варьироваться от временного нарушения управления системой до необратимого повреждения микросхем.

Необходимо контролировать параметры внешней среды (например, температуру, давление). Большое отклонение параметров от нормальных может привести к повреждению оборудования, например перегреву процессоров. Некоторые процессоры прекращают работу для собственной защиты, некоторые могут продолжать работу с минимальной производительностью, постоянно выдавая ошибки, перезагружаясь или вовсе выходя из строя.

Для критически важных компонентов АСУ необходимо создать систему резервного питания. Полное отключение питания может прекратить работу АСУ или привести к установке небезопасных настроек по умолчанию. В этой части рекомендации представлены в основном типичные уязвимости вычислительных систем, однако внимание акцентировано на уязвимостях, возникающих в связи с изменением температурных параметров, изменение которых может нанести существенный вред АСУ.

6. Уязвимости в разработке программного обеспечения. В АСУ может случиться так, что программные средства защиты установлены, но не включены. Чтобы избежать таких казусов, следует проверять активность ПО.

Программное обеспечение АСУ может неправильно проверять входные данные. Неверные данные могут привести ко многим уязвимостям, таким как переполнение буферов, инъекции, межсайтовый скриптинг и обход каталогов. Также следует ограничивать доступ к настройкам и программному обеспечению. Несанкционированный доступ может привести к повреждению оборудования.

7. Уязвимости в коммуникации и настройке сети. Современные АСУ соединены с другими системами или с открытыми сетями. Для ограничения передающейся информации необходим контроль потоков данных на основе их характеристик. Этот контроль может предотвратить утечку информации и нелегальные действия. Чтобы не позволять ненужным данным проходить между сетями, в системе должны быть правильно настроенные брандмауэры. Их отсутствие делает конфиденциальную информацию чувствительной к мониторингу и прослушиванию, а также предоставляет несанкционированный доступ к системе.

Злоумышленники, которые следят за сетевой активностью АСУ, могут использовать анализаторы протоколов и другие утилиты для декодирования данных, передаваемым по протоколам telnet, FTP и NFS. Использование таких протоколов облегчает злоумышленникам возможность атаковать АСУ и манипулировать сетевой активностью.

Многие протоколы АСУ не имеют механизмов аутентификации и шифрования. Без аутентификации существует вероятность воспроизведения, изменения или подмены данных. Надежная двусторонняя аутентификация необходима и в беспроводных сетях, чтобы исключить возможность подключения к мошенническим точкам доступа, а также исключить возможность подключения злоумышленников к беспроводной

сети АСУ. Конфиденциальная информация, передающаяся между клиентами и точками доступа, должна быть хорошо зашифрована, чтобы злоумышленники не могли получить доступ к незашифрованным данным. DNP 3.0, Modbus, Profibus и другие являются распространенными в нескольких отраслях промышленности протоколами, находящимися в открытом доступе. Данные протоколы не имеют ни механизмов аутентификации, ни шифрования. Кроме того, такие протоколы, как DNP и OPC, имеют многочисленные уязвимости.

Во многих промышленных протоколах управления отсутствует проверка целостности; злоумышленники могут использовать незамеченные подключения для изменения данных. Для обеспечения целостности АСУ могут использовать защищенные протоколы нижнего уровня (например, IPSec).

Для определения причин взлома АСУ должны иметь правильное и точное протоколирование.

Во многом уязвимости этой группы связаны с уязвимостями других групп. В частности, использование протоколов АСУ, не имеющих механизмов аутентификации и шифрования, свидетельствует о том, что требования безопасности не учитывались при разработке АСУ, что относится к уязвимостям, описанным в разделе 4.

Как видно из приведенного выше описания, уязвимости в АСУ могут возникать в самых разных частях системы.

О безопасности системы следует задумываться еще при ее проектировании, а если в будущем нужно будет провести какие-либо изменения, их нужно хорошо протестировать.

Большое число уязвимостей возникает из-за неправильной, непродуманной политики безопасности. Уязвимости могут проявляться в таких аспектах политики, как управление доступом, аутентификация, политика паролей, управление удаленным доступом и т.п. При непродуманной политике безопасности возникает большое количество непреднамеренных угроз, источниками которых являются сотрудники организации.

При разработке СБ АСУ ТП не следует забывать, что промышленные системы отличаются от традиционных IT-систем. Из классической связки «конфиденциальность–целостность–доступность» конфиденциальность отходит на второй план, а наиболее важными являются критерии целостности и доступности.

Также в описанных уязвимостях прослеживается необходимость в правильном и точном протоколировании. Оно может помочь определить слабости в системе безопасности или выявить причины взлома, если таковой произошел.

Выводы

Анализ уязвимостей на основе описания и классификации, представленных в документе NISTSP 800-82, позволит сравнить международный и российский опыт в области информационной безопасности АСУ ТП. Основными российскими документами, регламентирующими ИБ АСУ ТП помимо отраслевых законов [9, 10], является 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 и здоровья людей и для окружающей природной среды».

Американские стандарты по ИБ (в частности, NISTSP 800-82) опережают российские по уровню предъявляемых требований, а также качеству проработки самих стандартов и их связи с областью стандартов по информационной безопасности, поэтому сравнение информации, отраженной в документах, в том числе и выявление наиболее критичных уязвимостей, сопоставление мер по их предотвращению, разработка процессов и архитектур менеджмента безопасности будут представлять большой интерес для исследования.

На основании проделанной работы по анализу уязвимостей в дальнейшем будут оцениваться российские стандарты, предлагаемые ими методы и средства защиты АСУ.

Библиографический список

1. Гольд Р. Stuxnet: война 2.0 [Электронный ресурс]. – URL: http://habrahabr.ru/post/105964/ (дата обращения: 10.03.2016).

2. Волобуев П. Безопасность SCADA: Stuxnet – что это такое и как с этим бороться? [Электронный ресурс]. – URL: http://www.itsec.ru/articles2/Oborandteh/bezopasnost-scada-stuxnet-chto-eto-takoe-i-kak-s-etim-borotsya (дата обращения: 10.03.2016).

3. Базовая модель угроз безопасности информации в ключевых системах информационной инфраструктуры (утв. ФСТЭК России

18.05.2007) / Федеральная служба по техническому и экспортному контролю. – URL: http://www.fstec.ru/tekhnicheskaya-zashchita-informatsii/dokumenty/114-spetsialnye-normativnye-dokumenty/379-bazovaya-model-ugroz-bezopasnosti-personalnykh-dannykh-pri-ikh-obrabotke-v-informatsionnykh-sistemakh-personalnykh-dannykh-vypiska-fstek-rossii-2008-god (дата обращения: 10.03.2016).

4. Методика определения актуальных угроз безопасности информации в ключевых системах информационной инфраструктуры (утв. ФСТЭК России 18.05.2007) / Федеральная служба по техническому и экспортному контролю. – URL: http://www.fstec.ru/tekhnicheskaya-zashchita-informatsii/dokumenty/114-spetsialnye-normativnye-dokumenty/380-metodika-opredeleniya-aktualnykh-ugroz-bezopasnosti-personalnykh-dannykh-priikh-obrabotke-v-informatsionnykh-sistemakh-personalnykh-dannykh-fstek-rossii-2008-god (дата обращения: 10.03.2016).

5. NIST Special Publication 800-82. Revision 2 Final Public Draft. Guide to Industrial Control Systems (ICS) Security [Электронный ресурс] / National Institute of Standards and Technology. – URL: http://csrc.nist.gov/publications/drafts/800-82r2/sp800_82_r2_second_draft.pdf (дата обращения: 10.03.2016).

6. NIST Special Publication 800-53. Revision 4. Security and Privacy Controls for Federal Information Systems and Organizations [Электронный ресурс] / National Institute of Standards and Technology. – URL: http://nvlpubs.nist.gov/nistpubs/SpecialPublications/NIST.SP.800-53r4.pdf (дата обращения: 10.03.2016).

7. Ботвинкин П.В., Миронов А.Ю. Понятие о SCADA-системах и обоснование необходимости комплексного подхода к обеспечению их информационной и физической безопасности // Сборник научных трудов Sworld. – 2014. – Т. 10. – № 3. – С. 36.

8. Менгазетдинов Н.И., Полетыкин А.Г. Интеграция АСУ ТП и системы верхнего уровня АЭС-технологии и опыт ИПУ РАН. – М., 2015.

9. Федеральный закон № 256-ФЗ. О безопасности объектов топливно-энергетического комплекса // Российская газета. Федеральный выпуск. – 26 июля 2011. – № 5537.

10. Федеральный закон № 116-ФЗ. О промышленной безопасности опасных производственных объектов. Приложение 1 // Российская газета. Федеральный выпуск. – 27 июля 2005. – № 3831.

References

1. Gol'd R. Stuxnet: voina 2.0 [Stuxnet: War 2.0], available at: http://habrahabr.ru/post/105964/ (accessed 10 March 2016).

2. Volobuev P. Bezopasnost' SCADA: Stuxnet – chto eto takoe i kak s etim borot'sia? [Secure SCADA: Stuxnet – what it is and how to fight it?], available at: http://www.itsec.ru/articles2/Oborandteh/bezopasnost-scada-stuxnet-chto-eto-takoe-i-kak-s-etim-borotsya (accessed 10 March 2016).

3. Bazovaia model' ugroz bezopasnosti informatsii v kliuchevykh sistemakh informatsionnoi infrastruktury [The basic model of information security threats in key information infrastructure systems]. Federal'naia sluzhba po tekhnicheskomu i eksportnomu kontroliu, available at: http://www.fstec.ru/tekhnicheskaya-zashchita-informatsii/dokumenty/114-spetsialnye-normativnye-dokumenty/379-bazovaya-model-ugroz-bezopasnosti-personalnykh-dannykh-pri-ikh-obrabotke-v-informatsionnykh-sistemakh-personalnykh-dannykh-vypiska-fstek-rossii-2008-god (accessed 10 March 2016).

4. Metodika opredeleniia aktual'nykh ugroz bezopasnosti informatsii v kliuchevykh sistemakh informatsionnoi infrastruktury [Methods of determining the actual threats to the information security in key information infrastructure systems]. Federal'naia sluzhba po tekhnicheskomu i eksportnomu kontroliu, available at: http://www.fstec.ru/tekhnicheskaya-zashchita-informatsii/dokumenty/114-spetsialnye-normativnye-dokumenty/380-metodika-opredeleniya-aktualnykh-ugroz-bezopasnosti-personalnykh-dannykh-pri-ikh-obrabotke-v-informatsionnykh-sistemakh-personalnykh-dannykh-fstek-rossii-2008-god (accessed 10 March 2016).

5. NIST Special Publication 800-82. Revision 2 Final Public Draft. Guide to Industrial Control Systems (ICS) Security, available at: http://csrc.nist.gov/publications/drafts/800-2r2/sp800_82_r2_second_draft.pdf (accessed 10 March 2016).

6. NIST Special Publication 800-53. Revision 4. Security and Privacy Controls for Federal Information Systems and Organizations, available at: http://nvlpubs.nist.gov/nistpubs/SpecialPublications/NIST.SP.800-53r4.pdf (accessed 10 March 2016).

7. Botvinkin P.V., Mironov A.Iu. Poniatie o SCADA-sistemakh i obosnovanie neobkhodimosti kompleksnogo podkhoda k obespecheniiu ikh informatsionnoi i fizicheskoi bezopasnosti [The concept of SCADA-systems and the ststament of an integrated approach need to their information and physical security]. *Sbornik nauchnykh trudov Sworld*, 2014, vol. 10, no 3. 36 p.

8. Mengazetdinov N.I., Poletykin A.G. Integratsiia ASU TP i sistemy verkhnego urovnia AES-tekhnologii i opyt IPU RAN [The integration of automatic process control system and the system of the upper level of nuclear technology and the experience of Institute of Control Sciences RAS]. Moscow, 2015.

9. Federal'nyi zakon № 256-FZ. O bezopasnosti ob''ektov toplivno-energeticheskogo kompleksa [Federal Law № 256-FZ. On Safety of the Fuel and Energy Complex Facilities]. *Rossiiskaia gazeta. Federal'nyi vypusk*, 26 July 2011, no. 5537.

10. Federal'nyi zakon № 116-FZ. O promyshlennoi bezopasnosti opasnykh proizvodstvennykh ob''ektov. Prilozhenie 1 [Federal Law № 116-FZ. On Industrial safety of hazardous production facilities.Annex 1]. *Rossiiskaia gazeta. Federal'nyi vypus*, 27 July 2005, no. 3831.

Сведения об авторах

Бортник Дмитрий Аркадьевич (Пермь, Россия) – студент Пермского национального исследовательского политехнического университета. (614990, г. Пермь, Комсомольский пр., 29, e-mail: bortnikdmitriy@mail.ru).

Каменских Антон Николаевич (Пермь, Россия) – аспирант, ассистент кафедры автоматики и телемеханики Пермского национального исследовательского политехнического университета (614990, г. Пермь, Комсомольский пр., 29, e-mail: kamenskikh.anton@gmail.com).

About the authors

Bortnik Dmitriy Arkadievich (Perm, Russian Federation) is a Student Perm National Research Polytechnic University (614990, Perm, 29, Komsomolsky pr., e-mail: bortnikdmitriy@mail.ru).

Kamenskih Anton Nikolaevich (Perm, Russian Federation) is a Graduate Student, Assistant Lecturer at the Department of Automation and Telemechanics Perm National Research Polytechnic University (614990, Perm, 29, Komsomolsky pr., e-mail: antoshkinoinfo@yandex.ru).

Получено 20.02.2016