АВТОМАТИКА, КОМП'ЮТЕРНІ ТА ТЕЛЕКОМУНІКАЦІЙНІ ТЕХНОЛОГІЇ

УДК 621.565.94:004.2

Особенности информационной безопасности в электроэнергетике

Е. В. Смирнова[1], А. О. Смирнов[2], О. В. Ольшевская[3]
[1,3] Одесская национальная академия пищевых технологий, ул. Канатная,112, г. Одеса, 65039, Украина
ORCID: [1] 0000-0002-3818-8083, [2] 0000-0002-9459-6292, [3] 0000-0002-4512-3915
Scopus ID: [3] 57192687506
E-mail: [1] smirnova.kathrin@gmail.com , [2] smyrnov.aleksandr.dev@gmail.com , [3] olshevska.olga@gmail.com

Вопрос безопасности объектов критической важности, в частности в сфере электроэнергетики, всегда стоит остро как перед владельцами предприятий, так и перед государством. В статье рассматриваются особенности обеспечения информационной защиты для электроэнергетической области. Предложена концепция организации информационной безопасности автоматизированных систем управления технологическими процессами. Концепция затрагивает как электроэнергетические предприятия, так и промышленные предприятия в целом.

Ключевые слова: *Информационная безопасность; АСУ ТП; SCADA; Электроэнергетика.*

Особливості інформаційної безпеки в електроенергетиці

К. В. Смирнова [1], О. О. Смирнов [2], О. В. Ольшевська [3]
[1,3]Одеська національна академія харчових технологій, вул. Канатна,112, м. Одеса, 65039, Україна

Питання безпеки об'єктів критичної важливості, зокрема в сфері електроенергетики, завжди стоїть гостро як перед власниками підприємств, так і перед державою. У статті розглядаються особливості забезпечення інформаційного захисту для електроенергетичної галузі. Запропоновано концепцію організації інформаційної безпеки автоматизованих систем управління технологічними процесами. Концепція зачіпає як електроенергетичні підприємства, так і промислові підприємства в цілому.

Ключові слова: *Інформаційна безпека; АСУ ТП; SCADA; Електоенергетика.*

1. Введение

После известного инцидента с Stuxnet, а также недавних атак на энергетические объекты в Украине при помощи Black Energy, имевших серьезные последствия, вопрос защиты критически важных объектов, которые оснащены автоматизированными системами управления, не теряет своей актуальности. В условиях постоянного роста уязвимостей АСУ ТП остро ощущается нехватка специалистов в данной области. Проблема усугубляется еще и тем, что сами вендоры АСУ ТП недостаточно внимания уделяют безопасности своих продуктов, так как изначально системы были изолированы, и информационная защита не носила критический характер. Однако, в результате развития и удешевления техники, а также постоянного развития информационных технологий, за последнее десятилетие АСУ ТП получили более широкое распространение и вышли за рамки только крупного производства. Сейчас АСУ ТП применяются в абсолютно различных областях – от систем по типу «умный дом» до атомных электростанций.

Электроэнергетика – отрасль, которая требует особого внимания и продуманности, в том числе и в вопросах информационной безопасности. Конечно подход к обеспечению безопасности корпоративных систем и сетей не сильно отличается от подходов в других отраслях. Но требования к концепции защиты критически важных объектов должны быть максимально жесткими.

В статье рассматриваются особенности обеспечения информационной безопасности на объектах электроэнергетической области. Описываются основные проблемы безопасности автоматизированных систем управления технологическими процессами, в частности, SCADA-систем. Приводится статистика уязвимости различных компонентов АСУ ТП.

Исходя из особенностей рассматриваемой области предложена концепция организации информационной защиты на электроэнергетических предприятиях. Пред-

ложенная концепция затрагивает как общие вопросы безопасности, так и организацию защиты на уровне сети, а также на физическом уровне.

Сегмент электроэнергетики достаточно крупный на рынке информационной безопасности (ИБ). Энергетические предприятия относятся к объектам критически важной инфраструктуры – от их стабильной работы зависит как жизнь простых граждан, так и функционирование крупных предприятий. Поэтому проблема информационной безопасности в энергетической отрасли всегда является актуальной и привлекает к себе внимание экспертов

Многие объекты энергетической отрасли являются критически важными для государства. Абсолютно все предприятия отрасли содержат в своем составе автоматизированные системы управления технологическими процессами (АСУ ТП), которые, в свою очередь, требуют соответствующей защиты.

В обеспечении ИБ АСУ ТП есть ряд ключевых моментов. Во-первых, в большинстве своем АСУ ТП предприятия объединены в промышленные сети, связаны с офисными сетями, а многие имеют связь с Интернет. Во-вторых, необходима защита рабочих мест операторов и SCADA-серверов. Это касается запуска неразрешенных приложений, неучтенных внешних накопителей и других устройств, использования вредоносного программного обеспечения. В-третьих, необходима защита промышленных контроллеров от несанкционированного доступа к ним, от изменения исполняемого в них программного кода и от отправки некорректных команд.

По статистике ведущих антивирусных компаний за 2016 год в Украине только за декабрь 19% промышленных систем были подвержены различного рода атакам. Угрозы, в первую очередь, были связаны с сетевыми атаками и атаками на автоматизированные рабочие места (АРМ) пользователей. Например, в том же декабре 2016 года была проведена успешная атака на подстанцию “Северная”, когда вышедшая из строя вся система управления обесточила большую часть Киева. Проведенное расследование инцидента выявило, что злоумышленники, скорее всего, использовали троянскую программу BlackEnergy. Первая версия вредоносной программы появилась еще в 2007 году. После проникновения в систему она позволяет злоумышленникам провести оценку важности доступной информации по заранее определенным критериям. После этого программа копирует все данные на указанный злоумышленниками сервер и удаляет их на зараженных устройствах. Ряд инцидентов, связанных с BlackEnergy, были проведены через уязвимость в программе для презентаций PowerPoint (в том числе среди пострадавших были сотрудники НАТО, работники украинских правительственных организаций, энергетические компании в Польше).

Особое опасение экспертов вызывают атаки на ядерные объекты, в том числе атомные электростанции. В 2009 году червь Stuxnet через обычное флеш-устройство попал в сеть одного из атомных заводов Ирана и модифицировал управляющее программное обеспечение так, что произошел сбой калибрующей программы и центрифуги, войдя в резонанс, вышли из строя. Тем самым саботировав всю ядерную программу целого государства. В 2014 году южнокорейская энергетическая компания Hydro and Nuclear Power пострадала от фишинговой атаки. Злоумышленники отправили сотрудникам несколько тысяч вредоносных писем и похитили чертежи и инструкции по обслуживанию нескольких атомных реакторов. В конце июня 2017 года (на момент написания статьи) в Украине из-за вирусной атаки пострадало множество энергетических предприятий. В том числе в списке пострадавших значится Чернобыльская АЭС – была затронута вся система документооборота станции.

2. Аналитическая часть

Если говорить о защите объектов электроэнергетической области, то основным защищаемым объектом является, как правило, не только информация, но и технологический процесс. И рассматриваемая проблема касается не только возможной утечки информации, но и защиты от нарушения технологического процесса за счет реализации различного вида киберугроз. То есть система защиты должна строиться с учетом обеспечения целостности и доступности технологического процесса, а также автоматизированных систем управления.

Говоря о технологических объектах и их защите, необходимо учитывать специфику АСУ ТП, а также специализированных систем, применяемых в электроэнергетике.

Слабость защиты современных АСУ ТП демонстрируют постоянные технические аудиты, которые показывают наличие следующих проблем: отсутствие корректной сегментации промышленных и офисных сетей, использование “слабых” паролей, использование “вшитых” в оборудование паролей, отсутствие четкого разграничения прав пользователей системы, применение несанкционированного ПО и периферийного оборудования и, что самое главное, отсутствие в штате специалистов по обеспечению ИБ АСУ ТП.

Рассмотрим основные проблемы АСУ ТП в области информационной безопасности.

Достаточно часто разработчики АСУ ТП используют собственные протоколы передачи данных, которые не являются стандартизированными. Это же касается и специализированного программного обеспечения, в котором минимальные механизмы ИБ (разграничение доступа, аутентификация и т.д.) не соответствуют современным требованиям, а зачастую и вовсе отсутствуют.

При разработке технологических систем главным показателем качества является надежность. При этом тестирование разработанной системы с дополнительными средствами защиты производится крайне редко и разработчики часто отказываются производить техническую поддержку в случае введение дополнительных средств защиты.

Следующая проблема – отсутствие своевременного обновления. Многие технологические сети не имеют выхода в Интернет, но при этом собственная система обновлений не внедрена. С одной стороны такой подход оправдан, так как установка обновлений – это простои в работе и риск сбоя после обновления, что недопустимо на критически важных объектах. Но с другой

стороны, отсутствие своевременных обновлений влечет за собой увеличение рисков успешного применения кибератак, так как практически все найденные уязвимости можно просмотреть в открытых базах.

Внешний анализ уязвимостей (по открытым базам уязвимостей) компонентов АСУ ТП показывает, что за последние годы количество уязвимостей остается почти неизменным (рисунок 1). Это объясняется возросшим интересом производителей оборудования к своевременному выявлению и устранению уязвимостей.

Наибольшее количество уязвимостей относятся к таким типам, как отказ в обслуживании (DoS), удаленное выполнение кода (Code Execution) и переполнение буфера (Buffer Overflow). Эксплуатация таких уязвимостей злоумышленником может привести к отказу в работе какого-либо оборудования или к его несанкционированной эксплуатации, что недопустимо по отношению к АСУ ТП.

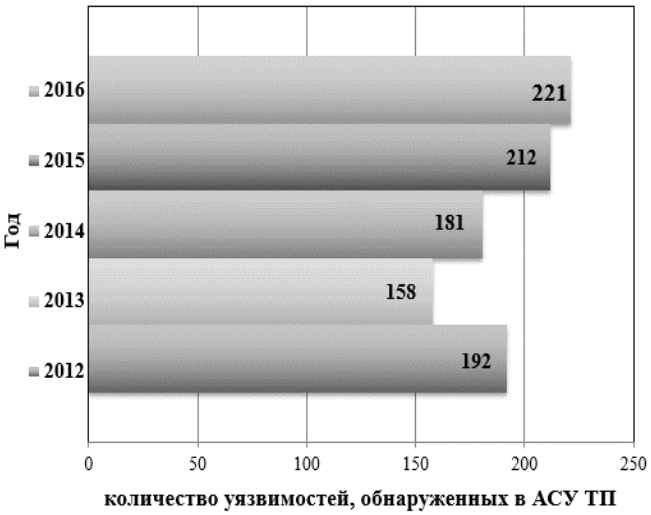

Рисунок 1 *– Динамика обнаружения уязвимостей АСУ ТП с 2012 по 2016 гг.*

Если рассматривать уязвимость отдельных компонент АСУ ТП, то особое внимание следует уделить безопасности SCADA. Как видно на рисунке 2, именно этот компонент на данный момент уязвим больше всего.

SCADA-системы используются во всех отраслях хозяйства, где требуется обеспечить операторский контроль за технологическими процессами в реальном времени.

С 2014 года произошел резкий рост вредоносного программного обеспечения, ориентированного на SCADA-системы. Для распространения трояна Havex в 2014 году злоумышленники производили взлом сайтов производителей ПО для управления промышленными предприятиями и заражали официальные дистрибутивы SCADA-систем. После установки таких зараженных систем на предприятиях, злоумышленникам удалось получить контроль над системами управления в нескольких европейских странах.

С чем связан такой рост уязвимостей SCADA-систем? Многие системы, управляющие производством (в том числе и энергоресурсами), можно найти в сети Интернет при помощи общедоступных поисковых систем. Причем владельцы систем чаще всего не осознают насколько доступными «снаружи» являются их системы и каким образом можно получить доступ к ним (например, через облачные сервисы, kiosk mode, через индустриальный wi-fi и т.д.).

Нередка ситуация, когда одна и та же SCADA-платформа используется для управления критически важными объектами в совершенно разных отраслях. Например, одна и та же система управляет адронным коллайдером, несколькими атомными электростанциями Ирана, химическими заводами, установками водоснабжения в Украине. Если уязвимость единожды найдена, злоумышленники могут атаковать множество различных объектов по всему миру.

Достаточно сложная организация АСУ ТП и требование непрерывности технологического процесса приводит к тому, что базовые компоненты систем управления устаревают, но не обновляются (о чем говорилось выше), а это приводит к повышенным рискам безопасности таким систем.

Еще одной немаловажной проблемой безопасности SCADA-систем является активное внедрение мобильных технологий во все сферы жизни. Сейчас можно отслеживать АСУ ТП и даже управлять ей прямо с мобильного телефона или планшета. Причем многие из подобных приложений разработаны производителями АСУ ТП, такими как Siemens, GE, Omron. Эти приложения обеспечивают доступ, контроль и управление HMI (человеко-машинный интерфейс), PLC (программируемый логический контроллер). DSC (распределенная система управления), SCADA в общей инфраструктуре АСУ ТП.

Насколько безопасно использование таких приложений? Клиент для SCADA позволяет инженерам-технологам подключаться с мобильного устройства к SCADA-приложению и при необходимости контролировать производственный процесс. Соединение между приложением и промышленным компонентом происходит в предположительно безопасной среде (на нижних и средних уровнях АСУ ТП). Поэтому отсутствие криптографии, аутентификации не относятся к категории высокого риска. Однако, если серверная часть приложения не проверяет корректность вводимых данных (с точки зрения промышленного процесса) или имеет уязвимости – о безопасности приложения речи идти уже не может.

Для SCADA-клиентов, исходя из существующих презентаций от разработчиков приложений, использование подразумевает удаленное управление снаружи промышленной сети. Это означает, что пользователи таких приложений могут подключаться к промышленному процессу из небезопасных общедоступных сетей, домашний сетей, используя мобильный интернет. Требования к безопасности и надежности таких приложений должны быть максимально строгими так как при помощи такого клиента возможны следующие угрозы: перехват и/или модификация трафика с целью компрометации технологического процесса, перехват и изменение управляющих команд, утечка критичной информации, Replay-атаки.

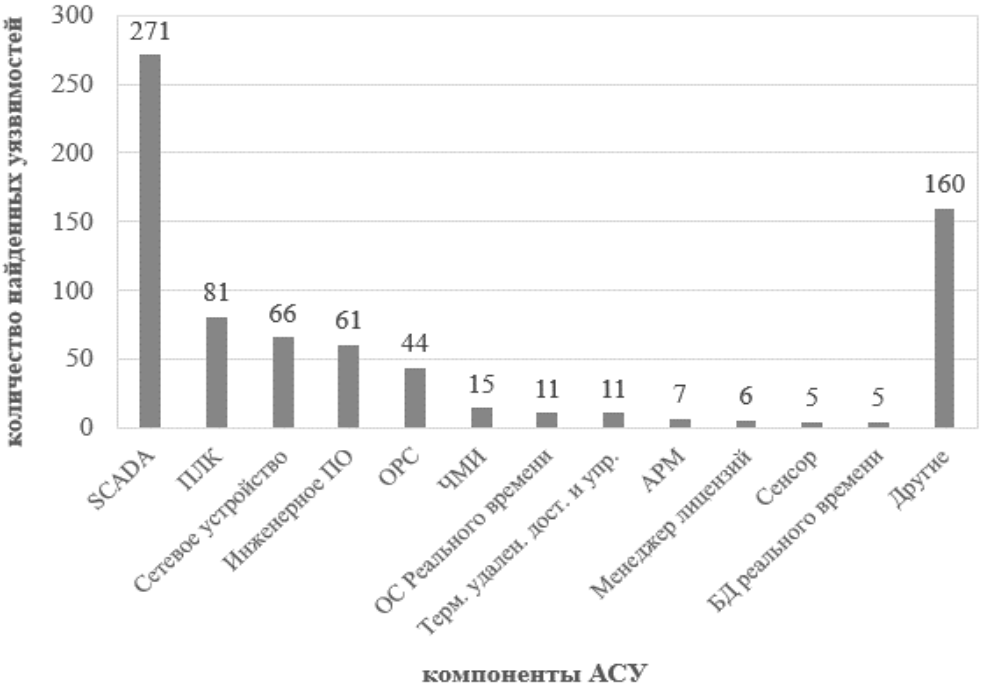

Рисунок 2 *– Уязвимости различных компонентов АСУ ТП*

3. Концепция организации информационной безопасности АСУ ТП

Целью ИБ является обеспечение надежного функционирования системы. Поэтому любое вмешательство (в том числе и надстройка по безопасности) не должно дестабилизировать работу. Применительно к области электроэнергетики сбой АСУ ТП, в большинстве случаев, вызовет цепную реакцию в нарушении функционирования промышленных потребителей электроэнергии. Чтобы избежать подобных инцидентов целесообразно разделить меры защиты как минимум на две категории: применимые в основном режиме работы и применимые только в технологическом режиме. Проводить сканирование сетей АСУ ТП для поиска уязвимостей, проводить обновление специализированного и системного ПО возможно только во время профилактики системы. Для основного режима работы необходимо спроектировать комплекс мер, которые обеспечат защиту от несанкционированного доступа во внутренние сети АСУ ТП, отследят потенциально опасные действия, отразят атаки извне.

Первым шагом в обеспечении мер безопасности необходимо пересмотреть организацию защиты АРМ. Необходимый минимум – это внедрение механизмов аутентификации, блокирования физических портов, контроль установленного ПО. Отдельным пунктом стоит обучение персонала культуре информационной безопасности. Наличие широких полномочий у сотрудников при доступе к АРМ управления порождает угрозу инсайдерских атак. Из этого вытекает необходимость постоянного мониторинга доступа как к АРМ, так и к специализированному ПО (доступ под обезличенной учетной записью, слишком короткие или слишком длинные сессии, доступ в запрещенное время).

В виду сложного и длительного цикла разработки специализированного ПО для АСУ ТП, обновления такого ПО выходят гораздо реже, нежели находятся бреши в его безопасности. На критически важных объектах одной из основных задач специалистов, отвечающих за обеспечение информационной безопасности, является сбор сведений об инфраструктуре АСУ ТП, существующих уязвимостях и сопоставление полученных данных с потенциальными угрозами.

Для предотвращения угроз на уровне сети необходим комплекс мер по обеспечению безопасности:

- отделить технологическую сеть от корпоративной и осуществлять мониторинг трафика внутри этих сетей, а также убедиться в том, что ни один член закрытой технологической сети не может иметь смежные доступы в любые другие, пусть тоже закрытые, сети;
- постоянный мониторинг таких сетей на предмет инородных и несвойственных им протоколов, создавая “белые” списки используемых протоколов конкретными SCADA-системами;
- отслеживать и записывать все ARP (Address Resolution Protocol – протокол определения адреса) и DNS (Domain Name System – система доменных имен) запросы для дальнейшего анализа их на предмет «отравляющих» (poisoning) и «обманывающих» (spoofing) атак;
- производить контроль времени и даты, отказаться от внешних NTP-серверов (Network Time Protocol – протокол сетевого времени);
- контролировать целостность и неизменность таблиц маршрутизации как управляющего маршрутизатора в этой сети, так и на конечных клиентах сети. В случае же если сеть не одноранговая, то и во всех маршрутизаторах, ответственных за свои фрагменты сети;

– производить контроль целостности файловой системы на всех клиентах сети, а также вести версионирование всего содержимого файловой системы;

– дополнительно целесообразно на защиту периметра такой сети поставить одну сигнатурную систему обнаружения вторжения для быстрого выявления шаблонных атак типа перегрузки буфера, а также более интеллектуальную эвристическую систему для защиты имеющихся веб-служб от всевозможных векторов атак свойственных данному протоколу.

Из физических мер необходимо:

– использовать только физический канал связи (например, хорошо экранированная витая пара) и ни в коем случае не прибегать к установке и использованию сетей и мостов на базе беспроводных технологий;

– любые порты доступа usb должны быть недоступными на физическом уровне;

– устройства ввода-вывода должны подключаться через ps/2 порт;

– должны отсутствовать CD и floppy диски, как и любые другие устройства вывода на носитель;

– ни в коем случае у клиентов, находящихся внутри этой сети, не должны использоваться беспроводные клавиатуры и мыши ввиду возможности легкого перехвата этих данных в эфире.

Также настоятельно рекомендуется обратить внимание на платформу, на которой базируется сервер для SCADA-системы и его проприетарные протоколы, зашитые туда вендором. Например, благодаря некачественному коду на платформах intel все процессоры, начиная с 2007 года, на чипсетах Intel от i5 до Xeon уязвимы к удаленному выполнению кода независимо от установленной операционной системы и наличия или отсутствия уязвимостей в программном обеспечении, так как уязвим, в данном конкретном случае, сам фундамент на котором стоит система.

Возможные схемы реализации основываются на функциях, доступных в технологии Intel AMT (Active Management Technology):

– KVM (удаленное управление мышью, клавиатурой и монитором) используется для удаленного выполнения любых физических операций (с мышью и клавиатурой), которые пользователи ежедневно делают на своем компьютере.

– IDE-R (IDE Redirection) используется для удаленного изменения загрузочного устройства на виртуальные образы. Таким образом, в системе будет загружаться операционная система не с жесткого диска, а с образа (виртуального диска) из источника, который указывается удаленно.

– SOL (Serial Over LAN) используется для удаленного включения/выключения/перезагрузки компьютера, а также выполнения других операций. Кроме того, при помощи этой функции можно менять настройки BIOS.

Выводы

Проведенный анализ показал, что количество уязвимых компонентов АСУ ТП из года в год практически не снижается. Большая часть уязвимостей, присущих современным АСУ ТП, можно отнести к критическим. Использование программных продуктов известных вендоров не является гарантом обеспечения надлежащего уровня информационной безопасности. Наиболее уязвимым компонентом являются SCADA-системы.

Достаточно часто в АСУ ТП используются словарные пароли и пароли по умолчанию, что позволяет легко получить к ним доступ и перехватить управление. Многие проблемы, относящиеся к безопасности внедренной АСУ ТП, вытекают из отсутствия в штате специалистов по ИБ еще на этапе проектирования системы.

Предлагаемая концепция обеспечения информационной защиты электроэнергетических предприятий максимально охватывает как общие вопросы безопасности, так и организацию защиты на уровне сети, а также на физическом уровне

Литература

1. **Грицай Г.** и др. Безопасность промышленных систем в цифрах [Электронный ресурс] // Сайт компании Positive Technologies. URL: http://www.ptsecurity.ru/download/SCADA_analytics_russian.pdf (дата обращения: 12.02. 2017). – 2012.

2. **Дружинин Е.** и др. Безопасность АСУ ТП в цифрах [Электронный ресурс] // Сайт компании Positive Technologies. URL: http://www. ptsecurity. ru/upload/ptru/analytics/ICS-Vulnerability-2016-rus.pdf (дата обращения: 17.02. 2017). – 2016.

3. **Марков А. С.** Организационно-технические проблемы защиты от целевых вредоносных программ типа Stuxnet [Текст] / А. С. Марков, А. А. Фадин // Вопросы кибербезопасности. – 2013. – №. 1.

4. **Остапенко А. Г.** Формализация процесса управления рисками в информационно-технологической инфраструктуре критически важного объекта [Текст] / А. Г. Остапенко, А. О. Калашников, Е. В. Ермилов, Н. Н. Корнеева // Информация и безопасность. – 2014. – Т. 17. – №. 2. – С. 164-179.

Отримана в редакції 05.04.2017, прийнята до друку 06.06.2017

Information Security Features in Electric Power Engineering

K. Smirnova[1], A. Smirnov[2], O. Olshevska[3]
[1,3] Odessa National Academy of Food Technologies, 112 Kanatna str., Odesa, 65039, Ukraine
ORCID: [1] 0000-0002-3818-8083, [2] 0000-0002-9459-6292, [3] 0000-0002-4512-3915
Scopus ID: [3] 57192687506
E-mail: [1] smirnova.kathrin@gmail.com, [2] smyrnov.aleksandr.dev@gmail.com, [3] olshevska.olga@gmail.com

The issue of critical importance objects safety, namely in the electric power engineering, is always acute both for the owners of enterprises and for the state. The article considers the features of providing information protection for the electric power engineering. The concept of organization of technological processes automated control systems information security is proposed. The concept touches upon both electric power enterprises and industrial enterprises as a whole.

Key words: *Information Security; Automated Control System; SCADA; Electric Power Engineering.*

References

1. **Hrytsai, H., Tymoryn, A., Holtsev, Iu., Ylyn, R., Hordeichyk, S. and Karpyn, A.** (2012) *Bezopasnost promyshlennykh system v tsyfrakh*, *Positive Technologies*. Available at: https://www.ptsecurity.com/upload/corporate/ru-ru/download/SCADA_analytics_russian.pdf (accessed 12 February 2017) (in Russian)
2. **Druzhynyn, E., Karpov, Y., Hnedyn, E., Boiko, Y., & Symonova, Iu.** (2016) *Bezopasnost ASU TP v tsyfrakh 2016*. Available at https://www.ptsecurity.com/upload/ptru/analytics/ICS-Vulnerability-2016-rus.pdf (accessed 17 February 2017) (in Russian)
3. **Markov, A. and Fadyn, A.** (2013) Orhanyzatsyonno-tekhnycheskye problemy zashchyty ot tselevykh vredonosnykh prohramm typa Stuxnet, *Voprosy kyberbezopasnosti*, No. 1 (in Russian)
4. **Ostapenko, A. H.** (2014) Formalizatsiia protsessa upravleniia riskami v informatsionno-tekhnolohicheskoi infrastrukture kriticheski vazhnoho obekta, *Informatsyia i bezopasnost*, 17 (2), 164–179 (in Russian)

Received 05 April 2017
Approved 06 June 2017
Available in Internet 03 July 2017