КИБЕРБЕЗОПАСНОСТЬ ПРОГРЕССИВНЫХ ПРОИЗВОДСТВЕННЫХ ТЕХНОЛОГИЙ В ЭПОХУ ЦИФРОВОЙ ТРАНСФОРМАЦИИ

Зегжда Д.П.[1], Васильев Ю.С.[2], Полтавцева М.А.[3], Кефели И.Ф.[4], Боровков А.И.[5]

Рассматриваются особенности четвертой промышленной революции, цифровую трансформацию управления производством, появление новых киберфизических систем. Приводится соответствующая трансформация систем управления информационной безопасностью. Рассматриваются новые угрозы цифровому производству, их особенности и каналы воздействия. Авторы предлагают подход к построению модуля управления информационной безопасностью цифрового производства на базе технологий мониторинга, оценки самоподобия и гомеостатического управления безопасностью, инвариантный к типу внешней угрозы.

***Ключевые слова**: цифровая трансформация производства, индустрия 4.0, угрозы цифрового производства*

DOI: 10.21681/2311-3456-2018-2-2-15

Введение

Изменения современного мира, вызванные бурны ростом с информационных технологий и всеобщей цифровизацией, не могли не затронуть производственные системы. Изобретение и повсеместное использование программируемых контроллеров, роботов и цифровых систем управления, интегрированных с корпоративными сетями предприятий, привело к изменению подходов к управлению производством, бурному развитию нескольких новых технологических управлений. Эта, так называемая «новая промышленная революция», не могла не найти отражение в задачах обеспечения безопасности промышленных систем.

Эволюция технологий и инструментов управления в сторону повсеместного применения компьютеризированных компонентов, вызвало появление и быстрый рост числа новых атак на промышленные системы. Современный злоумышленник использует целенаправленные атаки на объекты цифрового производства, специализированные арсеналы средств воздействия; не только технические методы, но, и, например, социальную инженерию.

В данной работе авторы рассматривают основные изменения в промышленных системах с появлением понятия «цифрового производства», трансформацию производственных процессов и подходов к обеспечению их безопасности при движении к цифровой экономике. Изменения в объекте защиты, или производственной системе, приводят к новым, целенаправленным атакам, расширению каналов воздействия. Новому классу угроз, названных, в соответствии с требованиями времени, «киберугрозами» ставится в соответствие новый класс систем обеспечения безопасности: систем кибербезопасности цифрового производства.

Технологическая эволюция производственных систем

Современное производство претерпевает существенные изменения в связи с повсеместным внедрением информационных технологий и систем. Электронными датчиками и контроллерами оборудуются практически все промышленные элементы и благодаря им в процесс организации потоков вещества и энергии при производстве добавляются еще и информационные потоки. В книге «Четвертая промышленная революция», декларировавшей эти изменения в 2016 году [1] подробно описывается процесс изменения экономики производства, вызванный стремитель-

1 Зегжда Дмитрий Петрович, доктор технических наук, профессор РАН, Санкт-Петербургский политехнический университет Петра Великого, Санкт – Петербург, Россия. E-mail: dmitry.zegzhda@ibks.ftk.spbstu.ru

2 Васильев Юрий Сергеевич, доктор технических наук., академик РАН, Санкт-Петербургский политехнический университет Петра Великого, Санкт – Петербург, Россия. E-mail:

3 Полтавцева Мария Анатольевна, кандидат технических наук, доцент, Санкт-Петербургский политехнический университет Петра Великого, Санкт – Петербург, Россия. E-mail: maria.poltavtseva@ibks.icc.spbstu.ru

4 Кефели Игорь Федорович доктор философских наук, директор Центра геополитической экспертизы и издательских проектов Северо-Западного института управления РАНХ, Санкт – Петербург, Россия. E-mail: geokefeli@mail.ru

5 Боровков Алексей Иванович, кандидат технических наук, доцент, Санкт-Петербургский политехнический университет Петра Великого, Санкт – Петербург, Россия. E-mail: Borovkov@CompMechLab.com

ными темпами технического развития, широтой применения информационно – телекоммуникационных технологий и системностью использования цифровых устройств. Термин «Индустрия 4.0», широко употребляющийся для обозначения новых производственных реалий, прозвучал впервые в 2011 году на Ганноверской ярмарке при обозначении процесса коренного преобразования глобальных цепочек создания стоимости [1,2]. Основной этого процесса стали технологии «умного» производства, оборудования, бытовых устройств. Сегодня гибкое взаимодействие различных физических систем посредством цифровых технологий меняет вид не только промышленности, но и экономики в целом.

Современный период называется «вторым машинным веком» [3], подчеркивая разницу между традиционными подходами использования аппаратного и программного обеспечения, неуклонно развивавшимися в течении всего двадцатого века, и новыми тенденциями, решениями глобальной компьютеризации и искусственного интеллекта. Несмотря на то, что программно-аппаратное управление появилось в производстве относительно давно, его применение в последние годы имеет существенные отличия:

Существенно возрастает масштаб проникновения цифровых технологий, как в различные отрасли и сферы деятельности, так и в отдельные производственные процессы.

Происходит синтез технологий, от расшифровки генома до нано технологий и систем возобновляемых энергоресурсов.

Стремительно возрастает скорость изменений - в отличие от предыдущих индустриальных революций промышленная революция 4.0 развивается не линейно, а по экспоненте [1].

Основную ценность общества «индустрии 4.0» представляет собой не продукция, а информация и потенциал информационного воздействия, за счет повсеместного использования автоматизации и обмена данными, компьютеризированных производственных систем, интернета вещей и облачных сервисов. По прогнозам, потенциал промышленного интернета вещей (IIOT, Industrial Internet of Things)[4], объединяющего сети физических объектов, платформ, систем и приложений со встроенными технологиями по обмену данных друг с другом, внешней средой и людьми, оценивается аналитиками более чем в тридцать триллионов долларов и продолжит возрастать [5].

Индустрия 4.0. характеризуется прорывом и бурным развитием нескольких областей технологий. Компания McKinsey группирует их в четыре категории[6], которые в развернутом виде представлены на рисунке 1.

***Рис. 1**. Технологии четвертой промышленной революции*

Все эти технологии напрямую связаны с цифровой трансформацией производства и новыми, киберфизическими системами. Они затрагивают как сами системы контроллеров и взаимодействующих промышленных устройств, так и смежные области. Ведущими направлениями развития, помимо собственно кибернетизации производства, аналитики [6] считают:

- Изменение интерфейсов АСУ, связанное с развитием графических интерфейсов, применением технологий touch-screen и технологий расширенной/виртуальной реальности. Несмотря на то, что бурное развитие этой области происходит в сегменте пользовательских устройств, его продвижение в область АСУТП тоже не за горами.

- Технологии обработки данных, генерируемых устройствами в процессе функционирования и взаимодействия. Согласно аналитическим отчетам [6], 40% таких данных никогда не сохранялась, а оставшиеся 60% хранятся короткое время, локально и почти не подвергаются анализу и обработке. Комплексный контроль цифрового производства требует сбора и обработки всей этой информации в центрах обработки данных и вычислительных системах.

- Технологии анализа данных и искусственного интеллекта находятся на вершине приведенного списка. Они необходимы для получения реальной выгоды от собранных и обработанных данных о производстве, оперативного и долговременного контроля и планирования производственного процесса. Итогом технологического рывка должны стать устойчивые к внешним изменениям, само адаптирующиеся производственные системы.

***Рис. 2.** Изменение производства в результате компьютеризации*

Объект защиты, понимаемый ранее как совокупность классифицированных данных, приобретает более сложное представление - как киберпространство, включающее не только данные, но и системы их передачи, обработки и хранения; системы управления; средства защиты; а также их динамически изменяющиеся взаимосвязи, составляющие определенную ценность. Сегментами киберпространства являются суперкомпьютеры, АСУ ТП, корпоративные и домашние сети, мобильные системы, облачные сервисы и даже социальные сети и бытовые устройства. Определим киберпространство как глобальную сферу в информационном пространстве, представляющую собой взаимосвязанную совокупность инфраструктур и информационных технологий, включая Интернет, телекоммуникационные сети, компьютерные системы, встроенные процессоры и контроллеры.

Трансформация производственной информатизации может быть представлена на рисунке 2, и сейчас можно говорить не о двух (старый и новый, киберфизический), а о трех этапах изменения промышленной среды. Первый включает в себя традиционные информационные системы и информационно-телекоммуникационные системы. Появление второго этапа вызвано кибернетизацией производственного процесса и повсеместным внедрением промышленных контроллеров. Третий – взгляд в будущее, уже озвучиваемый рядом специалистов [7,8]. Он предполагает цифровую интеграцию не только физических систем, но и организационных: кибернетизацию бизнес-процессов предприятий.

Сегодня происходит активное развитие киберфизических систем и переход к этапу интеграции с бизнес-процессами – цифровому производству и цифровой экономике. Формальные понятия киберфизических объектов и систем приведены в [9]. Киберфизической объект (КФО) – это концептуальная парадигма представления производственных, технологических схем в виде конгломерата средств преобразования различных видов материи и энергии и информационно-телекоммуникационной среды, обеспечивающей как обмен информацией между компонентами, так и устойчивое функционирование всей системы в условиях внешних воздействий с помощью автоматизированного управления. Киберфизические

системы (КФС) – можно определить, как наборы взаимодействующих киберфизических объектов, которые включают набор взаимосвязанных физических компонент, реализующих технологический процесс; информационных компонент, осуществляющих управление процессом в разной степени автоматизации; коммуникационную среду, обеспечивающая обмен информацией внутри системы и с окружающей средой и передачу управляющих команд исполнительным механизмом [9].

На этом этапе можно говорить о полном проникновении информационных технологий и применение их во всех сферах производственной деятельности, построение систем аддитивного производства, применения интеллектуальных роботов [10].

Например, Российская промышленность уже к 2020 году начнет использовать цифровые двойники реальных продуктов и производства. Введение на законодательном уровне разрешений на «цифровую сертификацию» продукции к 2020 году заложено в утвержденную правительством дорожную карту по снятию административных барьеров.

Цифровой двойник— это виртуальный образ реального объекта, который ведет себя на всех эксплуатационных режимах, включая нормальные условия и аварийные ситуации, так же, как и реальный объект. Он экономит разработчикам значительное количество времени и финансов на натурные испытания и перепроектирование продукции.

Специально организованный процесс «цифровой сертификации» позволит проводить разработку цифровой модели изделия на всех этапах жизненного цикла и виртуальные испытания на виртуальных стендах и полигонах, начиная от новых моделей автомобилей, ракет, самолетов и заканчивая кофеварками или пылесосами. После выполнения десятков тысяч виртуальных испытаний цифрового двойника кузов нового автомобиля, к примеру, достаточно испытать в натурных краштестах всего один раз, что резко ускоряет процесс производства и сертификации продукции[11].

Цифровая трансформация производственных технологий

Производственные системы в существенной степени претерпели изменения в результате компьютеризации. Можно выделить два обобщенных этапа производства, характерных как для традиционных, так и для современных, компьютеризированных систем индустрии 4.0 (рис. 3).

Первым этапом становится создание цифрового двойника промышленного продукта или изделия – для производственных систем это может быть компьютерная модель или 3D образ изделия в системах проектирования. В этом случае, производственные системы относительно локализованы и можно говорить о них, как о традиционных системах проектирования, к которым применимы общепринятые меры информационной безопасности: создание доверенной среды, контроль внешнего доступа и так далее.

Вторым этапом является современное аддитивное производство, в управлении которым также широко применяется вычислительная техника – как показано выше, интегрированная с внешней средой намного больше, чем это принято в традиционных решениях. В этом случае становится практически невозможно полностью контролировать или исключить внешние воздействия на производственную систему и возникает актуальная задача обеспечения устойчивости производственного процесса в условиях переменного множества различных внешних воздействий.

В дальнейшем в статье делается упор именно на безопасность аддитивного производства и управления производственным процессом, как новую область в сфере обеспечения безопасности промышленных систем.

Цифровое управление производством

Рассмотрим общую схему производства, характерную для современных промышленных систем,

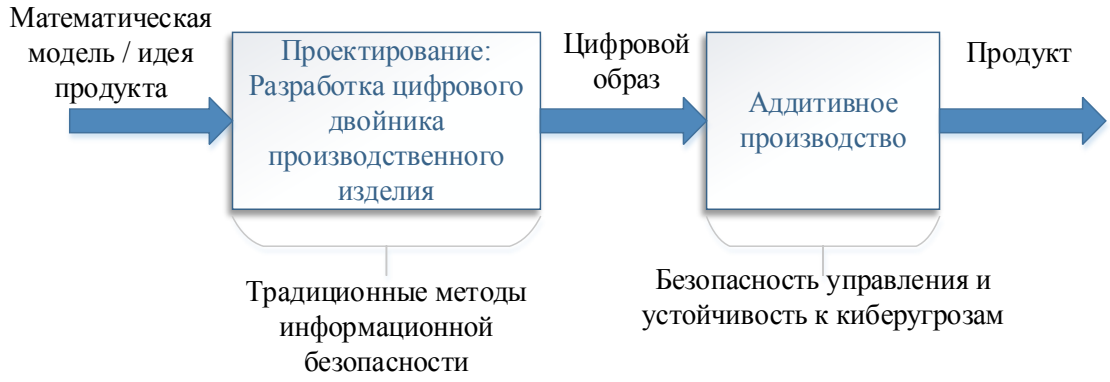

***Рис. 3**. Обобщенные этапы промышленного производства*

вступающих в эру цифровой экономики. В основе находятся системы управления физическими процессами, как и в предыдущем поколении производственных структур (рисунок 4). Над ними располагается управляющий слой контроллеров, осуществляющих сбор данных с физических объектов и генерирующих непосредственные управляющие воздействия, в соответствии с развернутым на них программным обеспечением. Контроллеры связаны в сети SCADA – систем, а те, в свою очередь, через общую коммуникационную среду – с корпоративной сетью предприятия. Необходимо отметить, что в качестве среды взаимодействия как правило выступает глобальная сеть (Internet).

Компьютеризация производства привела к слиянию исполнительных модулей и модулей взаимодействия систем, как следствие - к переходу к цифровому взаимодействию, обмену данными и управляющими командами. Если раньше каждый узел производственной системы представлял собой отдельный компонент с контуром управления, функция управления которого определялась в соответствии с теорией автоматизированного управления и типами обратных связей, сегодня такой узел не просто компьютеризирован, переведен на цифровое управление и сам по себе является киберфизическим объектом, но и активно взаимодействует с множеством других узлов, организуя производственный процесс практически без участия человека.

Понятие киберфизический объект (или системы как совокупности объектов) является удобной концептуальной схемой представления производственных и технологических схем, интегрирующих системы преобразования различных видов энергии и информационно-телекоммуникационную среду, обеспечивающую обмен между компонентами и устойчивое функционирование всей системы путем мониторинга и автоматизированного управления. Таким образом логическая концептуальная схема киберфизической системы, что также отражено на рисунке 3, включает:

- набор взаимосвязанных физических компонент, реализующих технологический процесс;
- набор взаимосвязанных информационных компонент, осуществляющих управление процессом в разной степени автоматизации;
- коммуникационную среду, обеспечивающую обмен информации внутри системы и с окружающей средой и передачи управляющих команд через ПЛК исполнительным механизмом.

Из-за сочетания физической, информационной и коммуникационной составляющих, в современной киберфизической системе функцией управления осуществляется через информационное воздействие, тогда как в традиционных системах автоматического управления и регулирования в основе функции управления лежала физическая величина. На основе киберфизических систем формируется киберсреда цифрового производства, которую можно описать как следующий набор компонент:

1. Центра управления;
   a. Корпоративной информационной среды;
   b. АСУ предприятия;
2. Обеспечения технологического процесса;
   a. АСУ технологических процессов (в общем случае всех протекающих на предприятии);

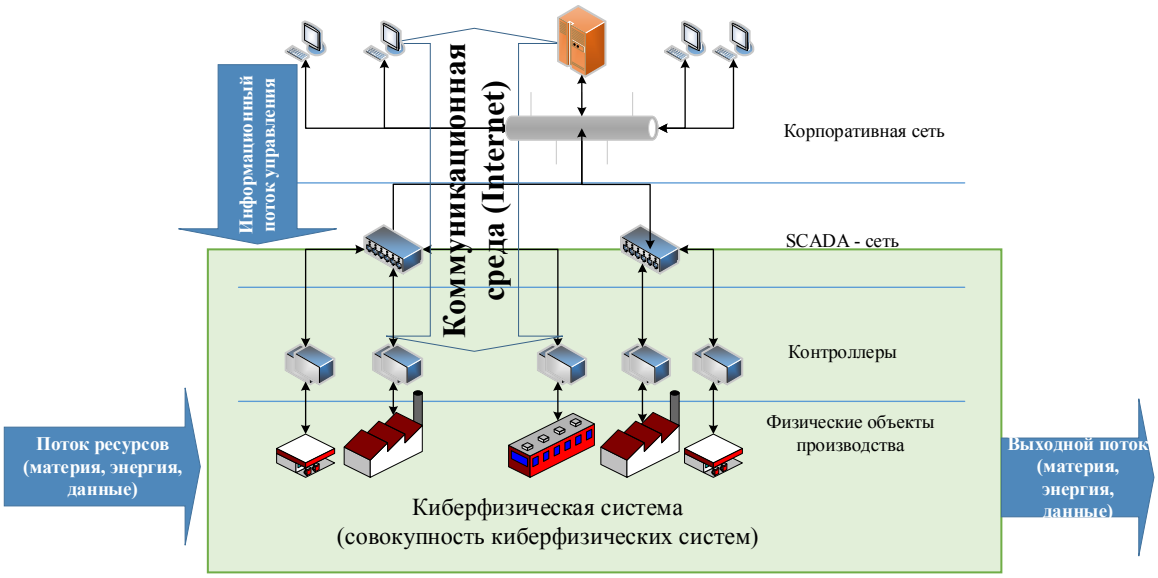

Рис. 4. *Общая схема цифрового производства*

b. Коммуникационной сети;

c. Физических компонент, реализующих процесс производства и управляемых программируемыми контроллерами;

d. Исполнительного механизма АСУТП.

3. Обеспечения безопасности производства;

a. Средств информационной безопасности;

b. Управления системами защиты.

Кифберфизическая система, исходя из концепции и особенностей такого рода систем [12], обладает следующими свойствами:

1. Наличие избыточности и резервирование ресурсов системы (допуская возможность пустого резервирования узлов).

2. Функциональная связность. Под функциональной связностью понимается способность создавать внутри системы целевые функции из комбинации ее отдельных узлов. Уровень декомпозиции функций в данном случае - есть глубина гомеостаза.

3. Возможность построения целевой функции (или функций) системы из заданного набора функций ее компонент.

Цифровизация промышленности привела к появлению в индустрии новых проблем, связанных с обеспечением информационной безопасности. Единое киберпространство, образуемое взаимодействующими системами на основе общих, универсальных протоколов и принципов удаленного управления, приводит к транзитивному замыканию всех действующих компонент, позволяя замкнуть через контуры цифрового взаимодействия все управляющие системы производственной, финансовой и социальной сферы. Глобальная доступность объектов киберпространства порождает проблему обеспечения устойчивой работы современного производства в условиях случайных и целенаправленных компьютерных атак, приводящих к долговременному и трудно обнаруживаемому воздействию на управление технологическими процессами.

Так изменяется само понятие и подход к безопасности АСУТП и производственных систем: возникает задача сохранения их работоспособности в условиях нового ландшафта угроз.

Угрозы безопасности цифрового производства

Особенностями инцидентов безопасности последних лет становится все больший рост серьезных инцидентов, связанных с АСУ ТП. Согласно распределению статистики кибератак осенью 2016 года, промышленность составляла больше 20% всех зафиксированных инцидентов, вместе с государством и военной отраслью уверенно превышая 50% всех атак. Доля таких областей, как социальные сети, файловые хостинги, новостные сайты, мобильные телекоммуникационные компании в совокупности составила менее 13% всех инцидентов.

Во многом рост атак на производственные системы связан с изменением их структуры, цифровизацией и появлением новых вызовов безопасности. Сегодняшний нарушитель, воздействуя через телекоммуникационные каналы или имея доступ к информационным ресурсам корпоративной сети предприятия имеет возможность оказывать влияние на производство в целом (рисунок 5).

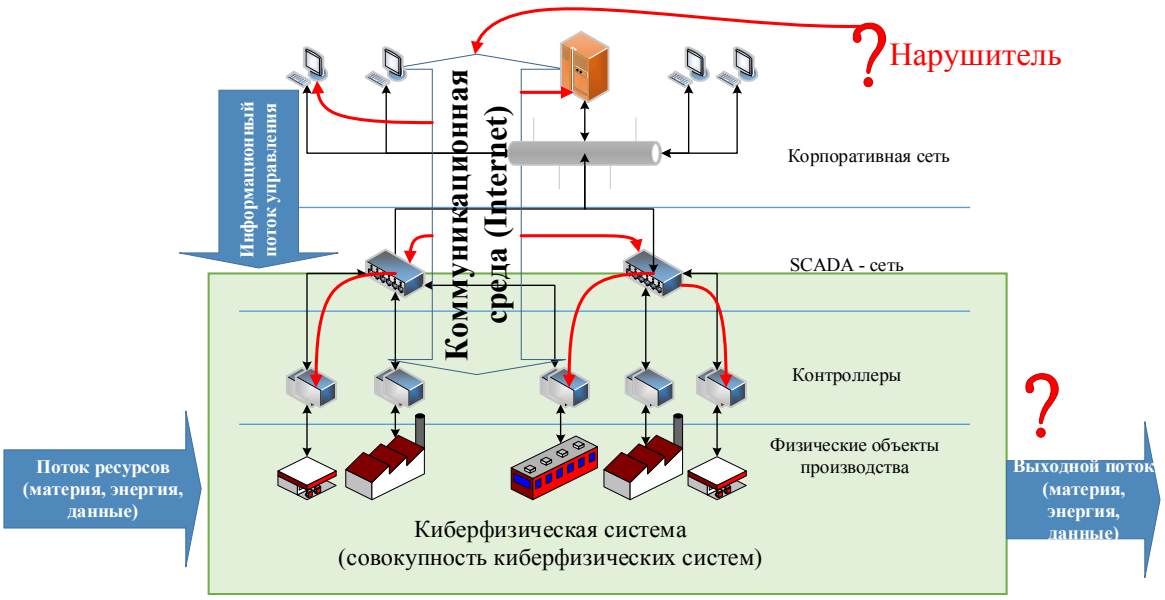

Рис. 5. *Новые возможности нарушения безопасности промышленного предприятия*

Второй важный момент – это возможность для нарушителя влиять через цифровые компоненты управления (сети и контроллеры) на материальный выход производственной системы, результат производственного процесса.

По данным SecurityLab.ru на 2015 год можно отметить получение злоумышленниками доступ к личным данным пользователей сервиса LastPass, и, таким образом, к множеству учетных данных в том числе, производственных систем. В качестве каналов проникновения по тем же данным в различных инцидентах использовались вирусы в изображения на легитимных web-сайтах; уязвимость, обнаруженная в смартфонах от Samsung; и даже электрическая интерференция в памяти DRAM.

Основные каналы воздействия, которыми может воспользоваться нарушитель, это воздействия на устройства; воздействия на подсистему управления; воздействие на протоколы и сетевое оборудование; воздействие на человеко-машинный интерфейс.

В рамках цифрового производства воздействия по всем приведенным каналам могут быть реализованы как информационные. Согласно статистике нарушений безопасности [13], в настоящее время происходит скачкообразный рост числа инцидентов АСУТП, связанных с их кибербезопасностью, и обусловленный тенденцией интеграции систем управления технологическими процессами и корпоративных информационных сетей (рисунок 6). Воздействия на автоматизированные системы управления технологическими процессами в почти 50% случаев уже происходят из корпоративной сети, а почти в 20% случаев – из сети Internet.

Согласно статистике, меняется общий характер атак на киберфизические системы. Характерными для цифрового производства становятся целенаправленные атаки, которые могут осуществляться транзитивно. За частую к их подготовке и проведению привлекаются специалисты в соответствующих промышленных отраслях и задействованном оборудовании. Злоумышленники используют сразу несколько методов и «векторов» атак, комплексный подход к реализации воздействия. Атаки включают в себя широкий набор не только технических методов, но и методов, основанных на социальной инженерии, психологии и т.д. Также новой является цель самой атаки – это не похищение информации, а воздействие непосредственно на происходящий технологический процесс. На сегодняшний день эта угроза зачастую оценивается более серьезно, чем похищение данных [7]. Отдельно необходимо отметить появление из-за информатизации дополнительных критических модулей и отставание нормативной базы.

Широкое использование облачных систем и систем с нечетким периметром, связано с развитием следующих угроз:

1) Угрозы, направленные на использование вычислительной мощности облака для решения

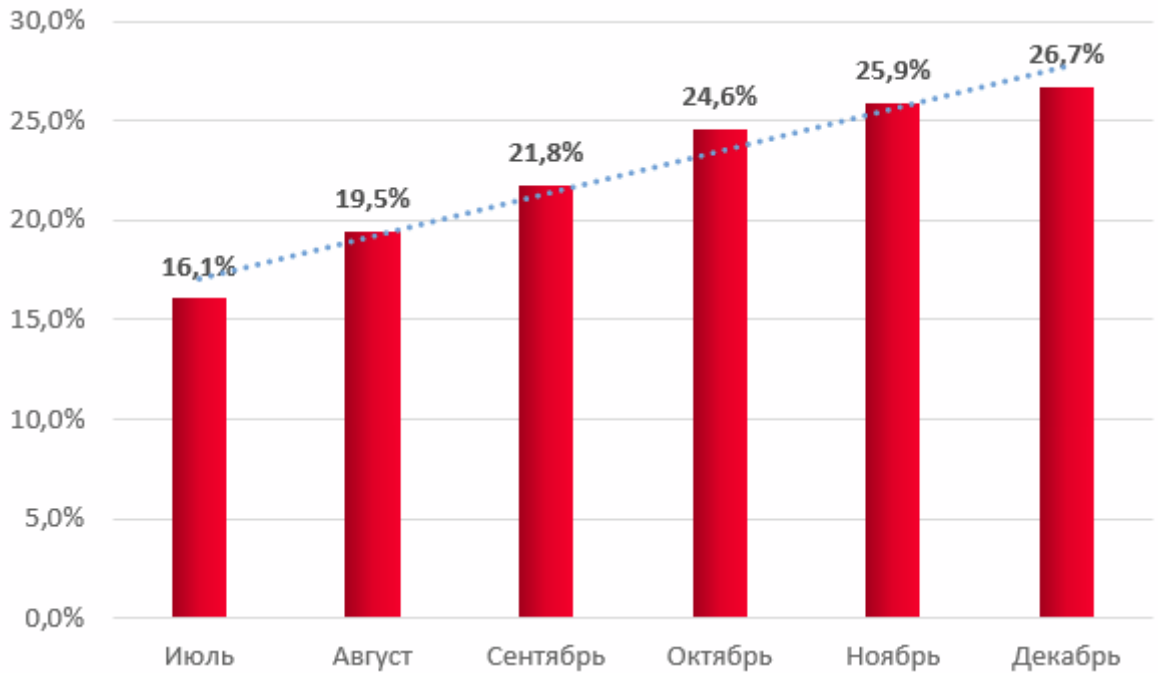

***Рис. 6**. Процент атакованных промышленных компьютеров в России за второе полугодие 2016-го года*

Таблица 1.
Систематизация угроз, возникающих в современных технологических системах

Технология	Уязвимые элементы	Последствия реализации угрозы	Особенности защиты
Виртуализация	Гипервизор	Захват управления	Защита «последней инстанции» – невозможно выявить успешную атаку
Облачные технологии	Механизмы разграничения доступа между ВМ	Разрушение структуры облака	Необходимость разграничения персональных ресурсов
Мобильные системы	Механизмы аутентификации и шифрования (не применяются или используются частично)	Перехват управления данными и использование для атак на связанные устройства	Недостаток энергоресурсов
«Умный дом»	Незащищенная связь с Internet, целостность ПО	Сбор критичной информации, вывод из строя, перехват управления	Невозможность интерактивного взаимодействия с пользователем

задач злоумышленника (например, brute force паролей и хэшей) или для маскировки источника воздействия на другие объекты.

2) Угрозы, направленные на платформы, инфраструктуры и ПО пользователей облака со стороны других пользователей облака или из сети Интернет.

Появление систем «умного дома», или в более общем виде появление понятия Интернет вещей, привело к возможности нарушения безопасности личного пространства в виде:

1) Использование бытовых устройств для проникновения на персональные компьютеры и мобильные телефоны.

2) Угроза жизни и здоровью пользователей (нарушение работы бытовых устройств может привести к пожарам, отравлениям и т.п.).

3) Подмена медиа-контента в качестве средства ведения информационных войн.

Угрозы безопасности SCADA определяется тем, что число подключенных к сети Интернет промышленных сетей растет – это обусловлено, в том числе, внедрением smart grid и «умных счетчиков», но многие из них по-прежнему используют изоляцию как основную меру защиты, а значит число и сложность атак на АСУ ТП возрастают. Систематизация новых угроз приедена в таблице 1.

Целью реализации современных киберугроз является вымогательство (при заражении CryptoLocker в сентябре 2013 г. пользователь либо теряет свои данные, либо вынужден платить злоумышленникам за расшифровку 2048-битного RSA ключа); промышленный шпионаж, для реализации которого используется программная инженерия; сбор персональных данных (в виде новой цели для атак, направленных на сбор персональной информации: повседневная активность, номера PIN для банковских карт, социальные данные и т.п.). Итогом рассмотрения новых горизонтов угроз является также появление новых целей в виде перехвата управления и навязывания своих алгоритмов управления; новых механизмов доставки ВПО: от поиска уязвимостей до социальной инженерии, целенаправленный выбор объекта атаки и планирование кибероперациий. Новыми целями атак становятся комплексные результаты: данные ® инфраструктура ® управляющие системы ® исполнительные механизмы.

Основные сложности при оценке и решении проблемы информационной безопасности современных производственных киберфизических систем, и, как следствие, цифрового производства, это:

- отсутствие должного внимания к проблеме;
- изменение характеристик воздействия;
- запаздывание нормативной базы.

Действительно, менее 2% от подвергшихся атакам предприятий сообщают об инцидентах, а специалисты АСУ ТП переоценивают степень защищённости своих систем: отсутствие подключения к интернету, возможности межсетевых экранов, безопасность систем противоаварийной защиты и их защищенность от внешнего воздействия.

Сочетание новых целей атак, таких как перехват управления и нарушение технологического процесса, новых механизмов проникновения и новых объектов атак приводит к необходимости новых подходов к обеспечению безопасности промышленных систем в эпоху цифрового производства.

Эволюция информационной безопасности производства

Информационная глобализация промышленности и энергетики в постиндустриальную эпоху проходит через несколько этапов, характеризующихся разной степенью передачи функций человека-оператора компьютерной системе. На ранних стадиях это выражалось степенью автоматизации производственной сферы, заключающейся, прежде всего, в автоматизации документооборота, процессов сбора и обработки информации и подготовки ее в соответствующем формате, для пользователя, принимающего решения или сохранении за человеком полного контроля над процессом.

Дальнейшая интеграция с компьютерными системами привела к постепенной передаче права формирования решений от человека-оператора к автоматизированной системе, что прежде всего было вызвано необходимостью максимально ускорить выполнение соответствующих действий или команд. Этот этап характерен интенсивным развитием методов и средств искусственного интеллекта, как тактики обоснования и оптимизации процесса принятия решений, что привело к созданию экспертных систем, нечеткого вывода, прогнозирующих систем и т.д.

Вместе с трансформацией традиционного производства (рисунок 2), происходит трансформация информационной безопасности (рисунок 7). С появлением киберфизических систем и интернета вещей, флагманов цифрового производства, к понятию информационной безопасности, базирующейся на безопасности информационно – телекоммуникационных систем, добавилось понятие кибербезопасности [14]. Разрабатываются оценки и методы обеспечения этого нового направления [14]. Также при интеграции с бизнес-процессами может произойти расширение традиционного понятия информационной безопасности еще на одну ступень. Какой она будет сегодня сказать еще трудно.

Природа цифрового производства обуславливает основную сложность, возникающую при создании модели угроз систем этого класса. Большое число пользователей, компонент, интеграция производства приводит к невозможности использования традиционных моделей атак, что видно на примере работ в области моделирования угроз современных промышленных систем (например, [15]). Предсказать и описать все многообразие возможных воздействий становиться трудно, если вообще возможно – а их число увеличивается по мере развития и интеграции технологий.

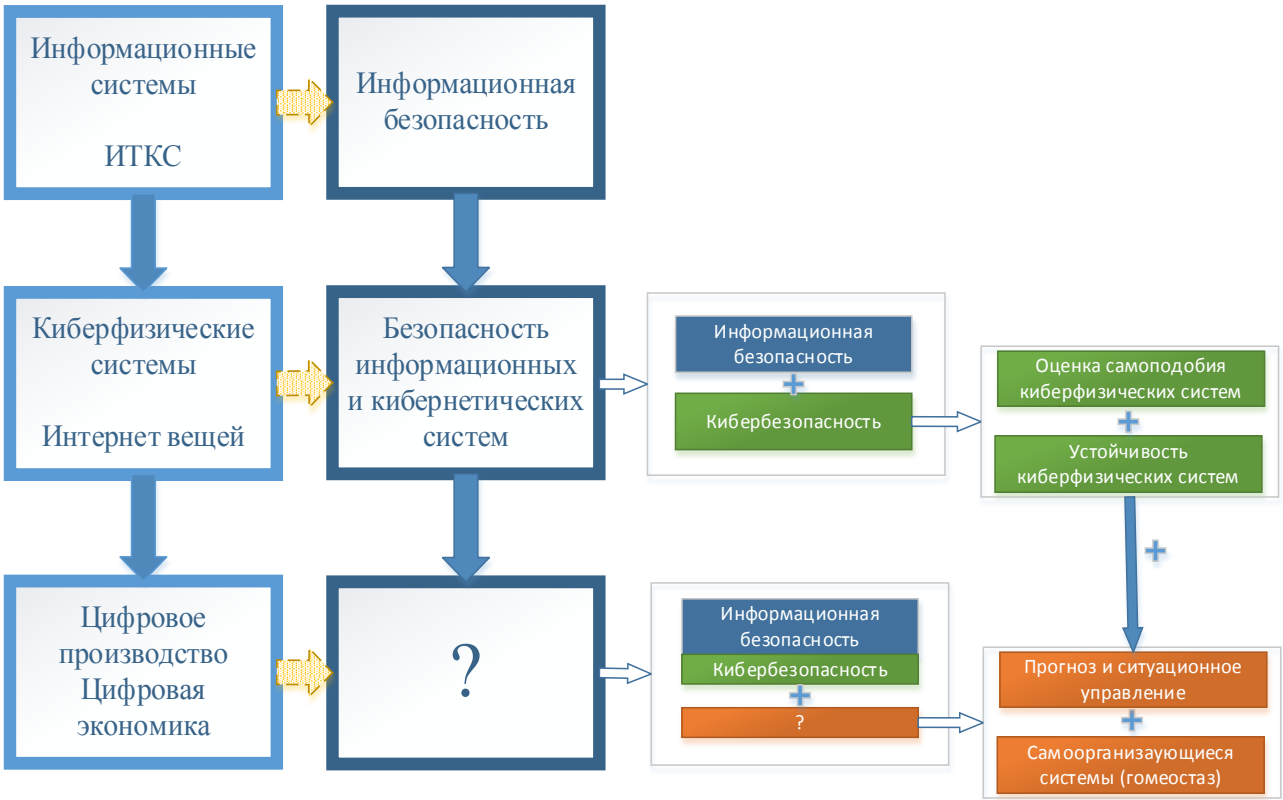

Рис. 7. *Трансформация понятия безопасности*

Кибербезопасность цифрового производства

Кибербезопасность — это набор принципов и средств обеспечения безопасности информационных процессов, подходов к управлению безопасностью и прочих технологий, которые используются для активного противодействия реализации киберугроз.

Задачи обеспечения кибербезопасности могут быть систематизированы как анализ механизмов нарушения защиты киберпространства, моделирование разрушающих воздействий; управление кибербезопасностью, определение зоны устойчивости объекта защиты, анализ киберрисков, разработка стандартов и нормативов безопасности киберпространства; синтез средств защиты киберпространства и контроль текущего состояния и функционирования компонентов киберпространства. В соответствии с этим современная парадигма обеспечения безопасности включает:

1. Пересмотр моделей управления доступом, учитывающих открытость, гибкость и распределенность. Модели должны быть основаны на темпоральной логике.

2. Принятие технологии виртуализации как мощнейшего средства защиты, которое позволяет перейти от понятия «защищенной системы» (от фиксированного множества угроз) к понятию «система с прогнозируемым поведением».

3. Реализация принципа разделения среды обработки информации и средств защиты.

4. Построение теоретических основ управления динамической защитой (адаптирующейся к текущим угрозам) как объекта автоматического регулирования с понятием зоны устойчивости, последействием (инерционностью) динамическими характеристиками

5. Принятие открытости систем (связь с Интернет) как неотъемлемого свойства и построение защиты с учетом этого:

6. Разработка основ оценки эластичности (настраиваемости системы) и масштабируемости.

Разработка новых принципов обнаружения атак, вирусов, руткитов, червей, РПС и прочего ВПО.

7. Учет возможности использования суперкомпьютеров для создания новых сценариев атак, систем сканирования, вмешательства в управление производством, криптоанализа. Учитывая, что мы вошли в эпоху кибервойн, суперкомпьютер - возможность создания нового оружия.

8. Анализ существующих тенденций развития средств обеспечения безопасности позволяет сделать вывод о смене парадигм защиты, базирующихся на технологиях защиты, которые условно могут быть определены как статическая, активная, адаптивная и динамическая. Идея такой классификации технологий защиты заимствована из теории управления. Несмотря на различие целей, преследуемых в теории управления и теории защиты информации, можно увидеть сходство подходов, используемых для достижения этих целей и направленных на удержание системы в границах некоторого набора состояний. При этом теория управления имеет более долгую историю развития и за счет этого – более богатую терминологическую базу. Множество критериев, на основе которых строятся классификации методов управления, обычно включает следующие параметры:

1. наличие обратной связи – в общем случае регуляторы с обратными связями могут использовать множество (больше одной) измеряемых величин и формировать несколько управляющих воздействий на регулируемый объект;

2. наличие контура адаптивного управления – надстраивается над контуром регулирования, назначение которого – подстраивать внутренние параметры регулятора так, чтобы достигался оптимум, характеризуемый определенным набором критериев – показателей качества;

3. наличие в контуре обратной связи функций прогнозирования состояния системы – на основании показателей, характеризующих систему и ее окружающую среду, строится множество условных сценариев, прогнозирующих развитие системы. Прогноз подается на вход регуляторов и влияет на формирование текущего управляющего воздействия.

На основе перечисленных критериев можно однозначно классифицировать существующие технологии защиты – для каждого из классов характерно наличие определенной совокупности перечисленных контуров. В статической технологии защиты функции управления не изменяется во времени, и режим работы описывается функциями зависимости выходного состояния объекта защиты от постоянных значений управляющих воздействий и других дестабилизирующих факторов, обратная связь, адаптивное управление и прогнозирование состояния системы отсутствуют. Активная технология защиты дополняет статическую введением обратной связи – результаты экспериментального тестирования объекта защиты используются для изменения настраиваемых параметров систем безопасности. Адаптивная технология защиты, соответственно, требует наличия

контура адаптивного управления – параметры систем безопасности периодически изменяется таким образом, чтобы показатели эффективности защиты (вычисляемые на основе характеристик объекта защиты в ходе мониторинга) стремились к максимуму. Заданная цель управления в рамках динамической технологии защиты – динамическая компенсация нежелательных изменений состояния системы «на лету» путем взаимодействия как с объектом защиты, так и с его инфраструктурой. Фундаментальным отличительным признаком динамической защиты является то, что защищаемая система трактуется системой защиты как нелинейный динамический объект с непрерывным временем, а сама система защиты становится дискретно-непрерывной.

Поэтому полное множество методов динамической защиты, лежащей в основе парадигмы кибербезопасности, включает методы изучения и влияния на окружающую среду изучаемого объекта, направленные на прогнозирование состояния системы в зависимости от динамики изменения внутренних и внешних (по отношению к защищаемой системе) факторов. Так мы приходим к понятию «система с прогнозируемым поведением» – для обеспечения кибербезопасности недостаточно описания состояния безопасности системы. Необходимо иметь возможность предсказать поведение системы в заданной (но неконтролируемой и недоверенной) окружающей среде, а в будущем – предсказать и динамику изменения внешних воздействий на защищаемую систему.

Это означает, что динамическая защита должна быть направлена на исследование не только защищаемой системы и механизмов реализации угроз, но и окружающей среды защищаемого объекта, и перспективных средств нарушения безопасности.

Авторы предлагают интегральный подход к обеспечению кибербезопасности, основной задачей которого является сохранение работоспособности системы цифрового производства в условиях различных целенаправленных воздействий. Эта концепция соответствует основному направление развития систем защиты сегодня – это реализации опережающей стратегии защиты: предчувствие угрозы и адаптация системы к будущему воздействию.

Общая схема цифрового производства с включением компонент безопасности представлена на рисунке 8. Блок обеспечения безопасности должен обеспечивать контроль основных параметров производственного процесса и проводить оценку безопасности текущего состояния системы опираясь на данные всех основных уровней: контроллеров, SCADA – сети и устройств, коммуникационной сети. Общий набор этапов функционирования блока безопасности соответствует позиции активной динамической защиты [14], чтобы соответствовать новым требованиям по необходимости прогнозирования воздействий. Это этапы мониторинга, оценки, принятия решения и выработки управляющего воздействия со стороны подсистемы обеспечения безопасности (если это необходимо).

Мониторинг реализуется набором методов и компонент, осуществляющих сбор и предварительную обработку данных о процессах, протекающих в системе цифрового производства, используя технологии обработки больших данных, методы нормализации и агрегации информации, интеграции сведений из различных источников.

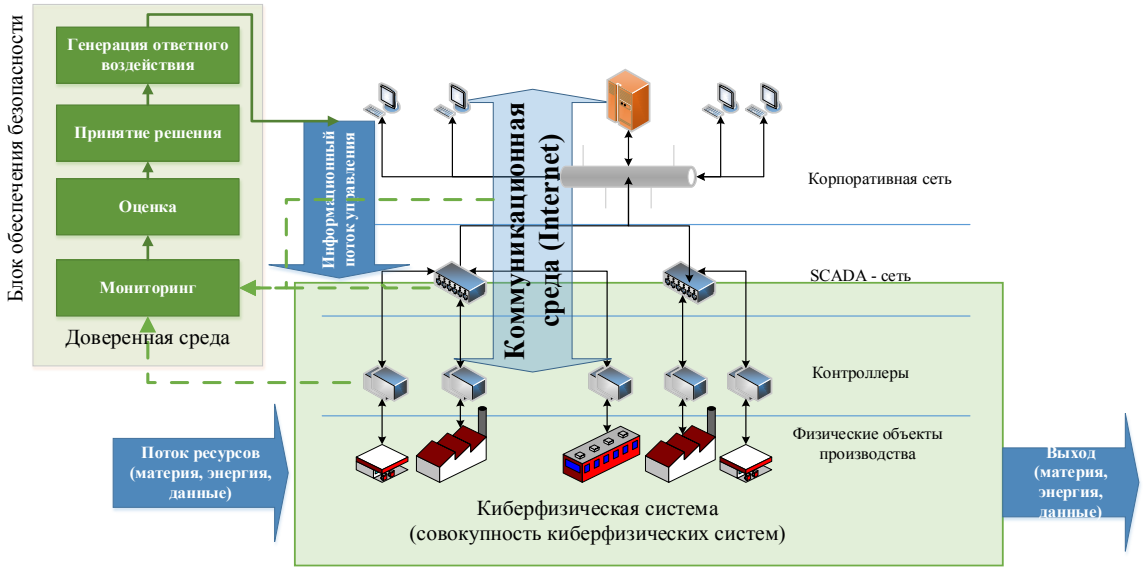

***Рис. 8**. Включение компонент безопасности в систему цифрового производства*

Оценка осуществляется через иерархию показателей устойчивости цифрового производства. Базовым является показатель самоподобия, отражающий текущее состояние системы. В зависимости от специфики данных и процесса, самоподобие может определяться на основе анализа корреляционных связей, показателя Херста, фактора Фано, фрактальных оценок [12]. Дополнительным важным компонентом является входящий в модуль оценки блок прогнозирования. Прогнозирование необходимо для анализа поведения системы в ближайшем интервале времени, оценки применимости тех или иных компенсирующих воздействий, так как каждое из них требует определенного времени реализации. Прогнозирование в системах цифрового производства основывается на технологиях анализа больших данных и методах оценки поведения динамических систем.

Устойчивость системы в целом определяется ее способностью к гомеостазу, то есть, способности к выработке и реализации компенсирующих воздействий [16]. Модуль принятия решения может строиться на одном или нескольких, примененных одновременно, подходах. Это выбор сценария из готовых в базе знаний, выработка компенсирующего воздействия на основании заложенных или полученных в результате машинного обучения правил, или другой механизм принятия решения. Основой для построения этого модуля должна стать теория ситуационного управления, основанная на оценке текущей ситуации и формировании варианта действий. Инструмент реализации выбранных сценариев и реакций уже присутствует в современных технологиях. Это программно-конфигурируемые и управляемые решения, например, программно – конфигурируемые сети.

Построенные по описанным принципам блок обеспечения безопасности будет способен проводить адекватную оценку ситуации, генерировать прогнозы ее развития, принимать и реализовывать решение о компенсирующем или опережающем воздействии при всем многообразии угроз цифровому производству.

Заключение

Авторами рассмотрены современные тенденции развития производственных систем, особенности цифрового производства и цифровой экономики, с точки зрения технологических изменений и изменений в области защищенности. Приведены основные технологии, легшие в основу индустриальных изменений и их влияние на производство и технологии защиты информации.

Цифровая трансформация производства, появление киберфизических объектов и систем, формирование киберсреды, является неизбежным следствием повсеместного использования программируемых контроллеров и компьютеризации процессов управления. Одновременно наблюдается рост и изменение специфики атак на производственные системы. Основными становятся APT (advanced persistent threat) атаки, целенаправленные, реализуемые группами злоумышленников, использующие различные технологии от специализированных программных решений до социальной инженерии, реализующие несколько «векторов» атак. Зачастую эти атаки направлены не на получение данных производственных систем, а на управление самим производственным процессом, контроль физических объектов. Новые атаки разнообразны и достаточно изобретательны, для больших гетерогенных систем цифрового производства все их многообразие становится трудно описать общепринятыми моделями. Злоумышленники используют широкий набор каналов воздействия, начиная от непосредственного влияния на оборудование, и заканчивая проникновением через корпоративные сети и общую коммуникационную среду.

В этих условиях важным направлением становится развитие кибербезопасности, как части информационной безопасности. Кибербезопасность объединяет подходы, методы и средства защиты киберфизических систем цифрового производства. Авторами предлагается интегрированный подход к защите, основанный на разработке защищенного модуля управления безопасностью. Основными компонентами модуля являются: блок мониторинга на базе технологий больших данных; блок инвариантной к угрозам оценки самоподобия системы и прогнозирования; блок выработки решения и блок управления гомеостазом. Успешное внедрение решений безопасности обеспечивается применением конфигурируемых компонентов и сетей (ПКС) в управлении технологическим процессом.

***Рецензент**: Сикарев Игорь Анатольевич, доктор технических наук, профессор, Государственный университет морского и речного флота имени адмирала С.О. Макарова, Москва, Россия E-mail: sikarev@yandex.ru*

Литература

1. Шваб К. Четвертая промышленная революция / К. Шваб — «Эксмо», 2016 — (Top Business Awards)
2. Официальный сайт Ганноверской ярмарки http://www.hannovermesse.de/home
3. Бринйолфссон Э., МакАфи Э. , «Вторая эра машин: работа, прогресс и процветание в эпоху блестящих технологий» / Э. Бринйолфссон, Э.МакАфи, Изд-во W. W. Norton & Company, 2014.
4. Industrial Internet of Things: Unleashing the Potential of Connected Products and Services // http://www3.weforum.org/docs/WEFUSA_IndustrialInternet_Report2015.pdf World Economic Forum 2015 REF 020315
5. Evans P. C., Annunziata M. Industrial Internet: Pushing the Boundaries of Minds and Machines // Peter C. Evans, Marco Annunziata November 26, 2012 http://files.gereports.com/wp-content/uploads/2012/11/ge-industrial-internet-vision-paper.pdf
6. Industry 4.0 How to navigate digitization of the manufacturing sector // McKinsey Digital 2015 http://www.cloud- finder.ch/fileadmin/Dateien/PDF/Themenkategorien/industrie40/McKinsey_Report_Industry_4.0_s.pdf
7. Анненков М. Основы киберустойчивости на финансовом рынке. // «!Безопасность Деловой Информации». Киберустойчивость. No 17 2017.
8. Акинин А. Киберустойчивость: веление времени // «! Безопасность Деловой Информации». Киберустойчивость. No 17 2017.
9. Васильев Ю.С. Проблемы безопасности цифрового производства и его устойчивость к киберугрозам // Ю.С. Васильев, Д.П. Зегжда, М.А. Полтавцева. Проблемы информационной безопасности. Компьютерные системы. 2017. № 4. С. 47-63.
10. Цифровое производство: методы, экосистемы, технологии. // Рабочий доклад Департамента Корпоративного обучения Московской школы управления СКОЛКОВО, Ноябрь 2017 года. http://odm3.io/
11. Промышленность начнет использовать цифровые двойники реальных изделий. // https://ria.ru/economy/20180410/1518265655.html
12. Зегжда П.Д., Систематизация киберфизических систем и оценка их безопасности // П.Д. Зегжда, М.А. Полтавцева, Д.С. Лаврова Проблемы информационной безопасности. Компьютерные системы. 2017. № 2. С. 127-138.
13. Безопасность АСУ ТП: Итоги 2017 года // ICS_Security_A4.RUS.0002.04.JAN.25.2018 https://www.ptsecurity.com/upload/corporate/ru-ru/analytics/ICS-Security-2017-rus.pdf
14. Zegzhda D.P. Sustainability as a criterion for information security in cyber-physical systems // Automatic Control and Computer Sciences. 2016. Т. 50. № 8. С. 813-819.
15. Дроботун Е. Б. Теоретические основы построения систем защиты от компьютерных атак для автоматизированных систем управления. Монография. – СПб.: Наукоемкие технологии, 2017. – 120 с.
16. D. P. Zegzhda E. Yu. Pavlenko Cyber-Physical System Homeostatic Security Management // Automatic Control and Computer Sciences ISSN 0146-4116. Vol. 51, No. 8, 2017

ADVANCED PRODUCTION TECHNOLOGES SECURITY IN THE ERA OF DIGITAL TRANSFORMATION

Zegzhda D.P.[6], Vasilev U.S.[7], Poltavtseva M.A.[8], Kefele I.F.[9], Borovkov A.I.[10]

In the article the authors examine the characteristics of the fourth industrial revolution, the digital transformation of the production management, the emergence of new cyber–physical systems. The corresponding transformation of information security management systems is given. New threats to digital production, their features and channels of influence are considered. The authors propose an approach to the construction of a digital production information security management module, based on monitoring technologies, self-similarity assessment and homeostatic security management, invariant to the type of external threat..

***Keywords**: digital transformation of production, industry 4.0, threats of digital production*

6 Zegzhda Dmitrii Petrovich Dr.Sc., Professor of RAS, Peter the Great St. Petersburg Polytechnic University, St. Petersburg, Russia. E-mail: dmitry.zegzhda@ibks.ftk.spbstu.ru

7 Vasilev Urii Sergeevich, Dr.Sc., Academician of RAS, Peter the Great St. Petersburg Polytechnic University, St. Petersburg, Russia.

8 Poltavtseva Maria Analolevna, Ph.D., Associate Professor, Peter the Great St. Petersburg Polytechnic University, St. Petersburg, Russia. E-mail: maria.poltavtseva@ibks.icc.spbstu.ru

9 Kefele Igor Fedorovich., Dr.Sc., Director of the center for geopolitical expertise and publishing projects of the North-West Institute of Management, branch of RANEPA, St. Petersburg, Russia. E-mail: geokefeli@mail.ru

10 Borovkov Aleksey Ivanovich, Ph.D., Associate Professor, Peter the Great St. Petersburg Polytechnic University, St. Petersburg, Russia. E-mail: Borovkov@CompMechLab.com

References

1. Shvab K. Chetvertaya promishlennaya revolutsia / K. Shvab — «Aksmo», 2016 — (Top Business Awards)
2. Official site Hannover messe http://www.hannovermesse.de/home
3. Briniiolfsson A., MacAffi A. «Vtoraya era mashin: rabota, progress i protsvetanie v epochy blestyashih technologii» / A. Briniiolfsson, A. MacAffi, W. W. Norton & Company, 2014.
4. Industrial Internet of Things: Unleashing the Potential of Connected Products and Services // http://www3.weforum.org/docs/WEFUSA_IndustrialInternet_Report2015.pdf World Economic Forum 2015 REF 020315
5. Evans P. C., Annunziata M. Industrial Internet: Pushing the Boundaries of Minds and Machines // Peter C. Evans, Marco Annunziata November 26, 2012 http://files.gereports.com/wp-content/uploads/2012/11/ge-industrial-internet-vision-paper.pdf
6. Industry 4.0 How to navigate digitization of the manufacturing sector // McKinsey Digital 2015 http://www.cloud-finder.ch/fileadmin/Dateien/PDF/Themenkategorien/industrie40/McKinsey_Report_Industry_4.0_s.pdf
7. Annenkov M. Osnovi kiberustoichivosti na finansovom rinke !Bezopasnost delovoi informatsii. Cyberustoichivost. No 17 2017.
8. Akinin A. Cyberustoichivost: velenie vremeni !Bezopasnost delovoi informatsii. Cyberustoichivost. No 17 2017.
9. Vasilev U.S., Zegzhda D.P., Poltavtseva M.A. Problemi bezopasnosti tsifrovogo proizvodstva i ego ustoichivost k cyberugrozam. Problemi informatsionnoi besopasnosti. Computer systems. 2017. № 4. P. 47-63.
10. Tsifrovoe proizvodstvo: methods, ecosystems, technologies. Rabochii doklad Departament corporativnogo obuchenia moscovskoi schkoli upravlenia SKOLKOVO, November 2017. http://odm3.io/
11. Promishlennost nachinaet ispolzovat tsifrovie dvoiniki realnich izdelii https://ria.ru/economy/20180410/1518265655.html
12. Zegzhda P.D., Poltavtseva M.A., Lavrova D.S. Systematizatsia cyberphizicheskih system i ozenka ih bezopasnosti Problemi informatsionnoi besopasnosti. Computer systems. 2017. № 2. P. 127-138.
13. Bezopasnost ACY TP: Itogi 2017 goda // ICS_Security_A4.RUS.0002.04.JAN.25.2018 https://www.ptsecurity.com/upload/corporate/ru-ru/analytics/ICS-Security-2017-rus.pdf
14. Zegzhda D.P. Sustainability as a criterion for information security in cyber-physical systems // Automatic Control and Computer Sciences. 2016. T. 50. № 8. P. 813-819.
15. Drobotyn E.B. Teoreticheskie osnovi postroenia systemi zachity ot computernih atak dlya avtomatizirovannich system upravlenia. SPb: Naukoemkie technologii, 2017. – 120 p.
16. D. P. Zegzhda E. Yu. Pavlenko Cyber-Physical System Homeostatic Security Management // Automatic Control and Computer Sciences ISSN 0146-4116. Vol. 51, No. 8, 2017