РАЗРАБОТКА МОДЕЛИ ПРОЦЕССА УПРАВЛЕНИЯ ИНФОРМАЦИОННОЙ БЕЗОПАСНОСТЬЮ КИБЕРФИЗИЧЕСКОЙ СИСТЕМЫ

DOI: 10.36724/2072-8735-2022-16-1-38-43

Грозмани Елена Сергеевна,
Санкт-Петербургский политехнический университет Петра Великого, аспирант, г. Санкт-Петербург, Россия,
grozmani.el@yandex.ru

Петров Сергей Вадимович,
Акционерное общество "Научно-исследовательский институт "Рубин", г. Санкт-Петербург, Россия,
grozmani.el@yandex.ru

Manuscript received 05 September 2021;
Accepted 16 November 2021

Ключевые слова: *киберфизические системы, информационная безопасность, менеджмент, модель, управленческое решение*

киберфизические системы (КФС) объединяют информационно-телекоммуникационные системы общего назначения и индустриальные сети и устройства (контроллеры), образуя гетерогенную иерархическую распределенную информационно-технологическую вычислительную среду, предназначенную для управления и мониторинга технологическими процессами. КФС активно внедряются в промышленную, городскую и бытовую сферы, позволяя обеспечить более эффективное использование ресурсов, а также перенести на новый уровень процессы управления и получения обратной связи. КФС формируются в результате агрегирования нескольких разнородных информационных и телекоммуникационных систем, что делает их восприимчивыми к деструктивным факторам цифровой среды – кибератакам. Особенности построения и функционирования КФС требуют нового подхода к определению поверхностей атаки и моделированию угроз. Это связано с тем, что "традиционные" цели злоумышленников – доступность, целостность и конфиденциальность обрабатываемой в системе информации не являются единственными. Кроме того, ценность самой информации может быть крайне низкой. В тоже время в киберфизической системе определяющую роль играют процессы управления и получения обратной связи. От их устойчивости напрямую зависит способность КФС выполнять целевые функции, а также физическая безопасность технологических объектов, персонала и потребителей. В зависимости от степени критичности технологических процессов реального мира, которыми управляет киберфизическая система, нарушение указанных потоков внутри нее может привести к серьезным последствиям, таким как большой материальный ущерб или угроза жизни и здоровью людей. Серьезность обозначенных угроз подтверждается постоянно растущим числом атак на КФС и последствиями, в том числе потенциальными, к которым данные атаки приводят. Дополнительно стоит отметить, что в условиях быстрого развития и совершенствования программируемых управляющих устройств (Programmable Logic Controller (PLC)), делающих их более доступными в массовом сегменте рынка, а также распространения высокоскоростных беспроводных сетей передачи данных, все более широкое применение получает концепция умного дома. Данный подход подразумевает интеграцию PLC, взаимодействующих друг с другом и центром управления посредством мультисервисных широкополосных беспроводных сетей, в бытовую среду. Таким образом, концепция умного дома строится на базе внедрения КФС в места постоянного проживания людей с передачей им функций автоматического управления климатическим оборудованием, освещением, бытовыми приборами, физическими элементами защиты от проникновений. При этом крайне важным является обеспечения информационной безопасности КФС. Для обеспечения требуемого уровня их защищенности, необходимо эффективно решать задачи управления процессом обеспечения их информационной безопасности. В статье предлагается подход к разработке модели процесса управления информационной безопасностью КФС, функционирующей в умном доме.

Информация об авторах:
Грозмани Елена Сергеевна, *Санкт-Петербургский политехнический университет Петра Великого, аспирант, г. Санкт-Петербург, Россия.*
Петров Сергей Вадимович, *Акционерное общество "Научно-исследовательский институт "Рубин", начальник отдела сертификационных испытаний, г. Санкт-Петербург, Россия.*

Для цитирования:
Грозмани Е.С., Петров С.В. Разработка модели процесса управления информационной безопасностью киберфизической системы // T-Comm: Телекоммуникации и транспорт. 2022. Том 16. №1. С. 38-43.

For citation:
Grozmani E.S., Petrov S.V. (2022) Development of cyber-physical system security management process model. *T-Comm*, vol. 16, no. 1, pp. 38-43. (*in Russian*)

Введение

Киберфизические системы объединяют информационные системы, телекоммуникационные среды передачи данных и программируемые устройства, предназначенные для управления и мониторинга техническими средствами. Являясь сложными гетерогенными системами, они обеспечивают высокоуровневые человеко-машинные интерфейсы, процессы хранения, обработки, включая анализ, и передачи больших массивов данных, а также контроля, проектирования и применения созданных моделей и параметров в управляемой среде. КФС реализует управление непосредственными исполнителями (электрические, гидравлические, термодинамические, климатические, роботизированные системы и комплексы и т. п.), а также осуществляется мониторинг и сбор данных, необходимых для реализации контроля, своевременно оповещения и выработки решений.

В тоже время, КФС можно рассматривать как концептуальную парадигму представления слияния процессов информационной и производственно-технологических сред в единую систему (конгломерат), обладающую способностью к преобразованию различных видов материи и энергии, а также информации, которая кроме того может обладать свойствами искусственного интеллекта. Важно отметить, что указанный конгломерат обладает способностью сохранять устойчивость функционирования в условиях переменной внешней среды благодаря наличию функций автоматического управления и контроля.

Практическими примерами киберфизических систем являются реализации концепций умного дома и интернета вещей (Internet of Things или IoT), системы управления производством (Industrial Control System или ICS), а также диспетчерского управления и сбора данных (Supervisory Control And Data Acquisition или SCADA). К географически распределенным КФС относятся системы контроля и управления движением. Примерами встраиваемых КФС выступают подсистемы современных автомобилей и сложного медицинского оборудования.

Киберфизические системы, интегрируя информационные системы и мультипротокольные вычислительные сети, могут быть подвергнуты кибератакам. В отличие от обычных информационных систем, предназначенных для обеспечения процессов обработки данных, основной задачей КФС является сохранение устойчивого функционирования управляемыми процессами реального мира. Это свойство определяет основные цели злоумышленников. Главной задачей атакующего является получение способности влияния на критически-важных информационные процессы внутри самой КФС. В первую очередь это процессы, обеспечивающие управление и мониторинг. При этом перехват контроля может не требоваться. Если конечной целью атакующего является разрушение физической среды, то может быть достаточно навязывания ложной информации либо блокирования каналов обратной связи. В результате изменения целей злоумышленников изменяются и последствия успешно реализованных атак. Для информационных систем это, как правило, финансовые и репутационные потери. В случае с КФС ущерб может быть намного более ощутимым, при этом нарушение работы или физическое разрушение производственной среды и/или технических средств могут создать угрозы здоровью и даже жизни людей. Ситуацию усложняет тот факт, что поверхность атак, проводимых на киберфизические системы, может быть значительно больше, чем у традиционных информационных систем. В нее могут входить системы управления производством, а также диспетчерского управления и сбора данных, которые проектировались для работы в изолированной среде и, как правило, не имеют адекватных механизмов защиты и внешних средств, позволяющих их обеспечить с учетом специфики данных систем. Сложность и гетерогенность КФС, наличие в их составе множества разнородных подсистем, взаимодействующих между собой, а также между компонентами с использованием специализированных протоколов, высокий потенциальный ущерб при успешной реализации атак на киберфизические системы требуют создания комплексной подсистемы обеспечения информационной безопасности, учитывающей специфику объекта защиты и характеристик деструктивных факторов внешней среды и их источников.

Подсистема обеспечения информационной безопасности является полностью либо частично независимой метасистемой по отношению к защищаемому объекту и представляет собой совокупность процессов, направленных на выявление и нейтрализацию угроз. На функционирование указанных процессов затрачивается определенное количество ресурсов, часть из которых является невосполнимой (в первую очередь время). Поэтому крайне важно обеспечить эффективность процесса обеспечения информационной безопасности. Кроме того, проведение успешных атак против киберфизических систем может создать угрозы здоровью и жизни людей. Это требует отдельного рассмотрения процесса управления информационной безопасностью. Большинство исследований посвящено именно процессам обеспечения информационной безопасности, а не управлению ими. В то же время в условиях ограниченности ресурсов отсутствие командных решений, адекватных реальной обстановке, не позволит обеспечить достижение целевых задач подсистемы обеспечения информационной безопасности.

Другой важной проблемой является обеспечения построения подсистемы управления информационной безопасности КФС с наперед заданными свойствами, способной обеспечить требуемый уровень защищенности. Для ее решения необходимо построение математической модели системы, которая бы позволила оценить характеристику прототипа еще до его создания. В настоящее время превалирующим подходом является построение моделей на основе анализа. Обладая рядом преимуществ, данных подход не в состоянии обеспечить построение систем с наперед определенными свойствами. Это обусловлено тем, что при его использовании не учитываются все закономерности и условия существования целевых процессов внутри моделируемой системы. Таким образом, создаваемые на основе таких моделей системы не могут обеспечивать устойчивое функционирование целевых процессов в условиях неопределенных и постоянно-меняющихся деструктивных факторов внешней среды. Эти же недостатки присущи и процессам управления обеспечения информационной безопасностью, моделируемым с помощью подхода на основе анализа.

Учитывая вышеизложенное, обеспечение безопасного функционирования киберфизических систем является приоритетной задачей в условиях их быстрого развития и по-

всеместного внедрения. В тоже время современные подходы к организации и обеспечению процессов управления безопасностью КФС не позволяют достигнуть целей управления с гарантированным результатом. Это создает угрозы возникновения неприемлемого ущерба.

Целью данного исследования является разработка модели процесса управления информационной безопасностью КФС, позволяющей получить гарантированный результат. В качестве объекта, на котором апробировался предложенный подход, был использован умный дом.

Предлагаемая методология

Процесс управления строится на выдаче командных решений. В свою очередь данные решения основываются на модели процесса управления, а также обеспечивающей его системы. При отсутствии адекватной модели процесса управления выработка корректных своевременных командных решений, соответствующих объективной обстановке, становится невозможной. Под адекватностью модели будем понимать ее свойство учитывать и отражать закономерности и ключевые характеристики объекта, которому она соответствует, а также процессов, протекающих в нем. Так как процесс управления должен быть непрерывным, его модель в первую очередь должна определять условия существования данного процесса. От успешного решения указанной задачи зависит адекватность модели в целом.

Выработку командных решений осуществляет лицо, принимающее решения (ЛПР). Это может быть конкретный человек либо группа людей или информационно-управляющая система, которая даже при наличии свойств искусственного интеллекта, является воплощением идей ее разработчиков [1, 2], основанных на их понятийно-логическом аппарате. Процесс выработки решения не является атомарной операцией. Он включает в себя несколько этапов, которые необходимо рассматривать одновременно в нескольких измерениях. В первую очередь ЛПР должно произвести декомпозицию решаемой задачи для разделения ее на полностью или относительно независимые части (блоки), каждая из которых может быть решена известными системе методами.

Далее происходит абстрагирование или формализация полученных промежуточных результатов. При этом происходит выделение определенных значимых в контексте решаемой задачи признаков и критериев с фиксацией значений их свойств за счет чего обеспечивается переход к требуемому уровню абстракции. После завершения предыдущего этапа осуществляется агрегирование полученных результатов с возможностью их интегральной оценки и получения необходимых выводов (решения). В случае, если система обладает свойствами искусственного интеллекта, то она может осуществлять накопление, полученных в результате указанных процессов результатов, и строить выводы из ранее неизвестных входных данных на базе уже имеющегося «опыта», а также вырабатывать новые закономерности.

Как было отмечено ранее, модель процесса управления обязательно должна определять условия его существования. Для выработки данных условий был использован закон сохранения целостности объекта [1, 2]. Он выражается в определении устойчивой связи (трансформации) свойств объекта и свойств его действия при фиксированном предназначении. В контексте рассматриваемого нами процесса объект трансформируется в обстановку, действие в информационно аналитическую работу, а предназначение в управленческое решение. Под управленческим решением будем понимать выдачу команд на применение ресурсов системы для обеспечения условий реализации предназначения объекта управления в соответствующей адекватной обстановке в интересах достижения целей управления. Обстановка – совокупность факторов и условий, в которых осуществляется деятельность. Информационно-аналитическая работа – непрерывный процесс получения требуемых сведений об обстановке [1, 2, 3]. На основе вышеуказанных процессов и закона сохранения целостности объекта можно осуществить синтез модели процесса управленческого решения в ее первом приближении. Графическое представление модели приведено на рисунке 1.

Рис. 1. Структурная схема интерпретации процесса синтеза математической модели решения

На первом уровне, применяя метод декомпозиции, расчленяем решение именно на три элемента обстановка, решение и информационно-аналитическая работа, которые соответствуют объекту, предназначению и действию. Применяя на втором уровне метод абстрагирования (формализации), мы отождествляем объект (обстановка) с периодичностью проявления проблемы для системы – Δt_{PM}, требующей выработки решения. Предназначение (решение) отождествляем с периодичностью нейтрализации проблемы (средним временем адекватного реагирования на проблему) – Δt_{PN}. Действие (информационно-аналитическая работа) отождествляем с периодичностью идентификации проблемы (средним временем распознания неблагоприятной ситуации) – Δt_{PI} [3]. Оперирование именно временными показателями обоснованно тем, что только данный ресурс является невосполнимым и имеет критическое значение в контексте обеспечения информационной безопасности. Также результаты исследований академика АН СССР Анохина П. К. [4], обобщенные им в теории функциональных систем, доказывают, что решение ЛПР формируется по схеме возбуждение, распознание, реакция на обстановку, что подтверждает корректность предлагаемого подхода. В работе используется следующая диаграмма выражения базовых компонентов формирования модели решения:

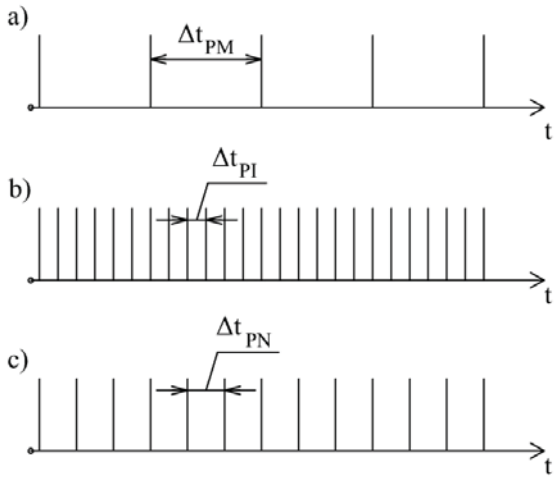

Рис. 2. Диаграмма проявления базовых элементов формирования модели решения

Путем агрегирования формализованных на предыдущем шаге критериев определятся математическая модель управленческого решения, которую можно представить в следующем виде:

$$P = F(\Delta t_{PM}, \Delta t_{PI}, \Delta t_{PN}) \quad (1)$$

Предлагаемый метод

В силу того, что базовая модель управленческого решения имеет три элемента, представим структурную схему управления следующим образом:

Рис. 3. Структурная схема управления

где, λ – величина, обратная среднему времени возникновения угрозы информационной безопасности; v1 – величина, обратная среднему времени выявления угрозы; v2 – величина, обратная среднему времени нейтрализации угрозы.

ЛПР, выраженное в виде информационно-командной системы, должно обеспечить выполнение условий существования целевых процессов в условиях неблагоприятной внешней обстановки путем выполнения следующих задач:

а) идентификация (распознавание) угрозы/проблемы;
б) нейтрализация (реагирование) угрозы/проблемы.

В связи с этим можно выделить четыре базовых состояния ЛПР [5, 6]:

A_{00} – ЛПР не идентифицирует и не нейтрализует;
A_{10} – ЛПР идентифицирует и не нейтрализует;
A_{01} – ЛПР не идентифицирует и нейтрализует;
A_{11} – ЛПР идентифицирует и нейтрализует.

P_{00}, P_{10}, P_{01}, P_{11} – вероятности нахождения в этих состояниях соответственно.

Для определения количественных целевых показателей необходимо составить систему дифференциальных уравнений Колмогорова, которые связывают вероятности нахождения системы в различных состояниях, при этом эти уравнения работают не с абсолютными интервалами (время), а с относительными – частотами (обратно пропорциональны времени).

Итак, рассмотрим граф состояний информационно-управляющей системы:

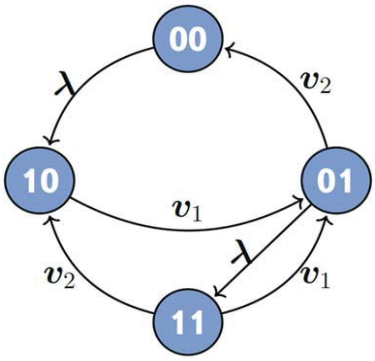

Рис. 4. Граф состояний информационно-командной подсистемы

где, λ – интенсивность проявления проблемы ($1/\Delta t_{PM}$); υ1 – интенсивность идентификации проблемы ($1/\Delta t_{PI}$); υ2 – интенсивность нейтрализации проблемы ($1/\Delta t_{PN}$).

Составим систему дифференциальных уравнений Колмогорова:

$$\frac{d}{dt}P_{00}(t) = -P_{00}(t)\lambda + P_{01}(t)\nu_2$$
$$\frac{d}{dt}P_{01}(t) = -P_{01}(t)(\lambda + \nu_2) + P_{11}(t)\nu_1 + P_{10}(t)\nu_1$$
$$\frac{d}{dt}P_{10}(t) = P_{00}(t)\lambda - P_{10}(t)\nu_1 + P_{11}(t)\nu_2$$
$$\frac{d}{dt}P_{11}(t) = P_{01}(t)\lambda - P_{11}(t)(\nu_1 + \nu_2) \quad (2)$$

Переход от дифференциальных уравнений к алгебраическим возможен при допущении, что переходные процессы отсутствуют, тогда производные $\frac{d}{dt}P_{00}(t) = 0$ (по условию постоянства функции) Кроме того сумма всех вероятностей равна единице: $P_{00}+P_{01}+P_{10}+P_{11}=1$.

$$-P_{00}(t)\lambda - P_{01}(t)\nu_2 = 0;$$
$$-P_{01}(t)(\lambda - \nu_2) - P_{11}(t)\nu_1 - P_{10}(t)\nu_1 = 0;$$
$$P_{00}(t)\lambda - P_{10}(t)\nu_1 - P_{11}(t)\nu_2 = 0;$$
$$P_{01}(t)\lambda - P_{11}(t)(\nu_1 - \nu_2) = 0. \quad (3)$$

Искомые вероятности уже не зависят от времени. Решением линейной алгебраической системы уравнений (3) является следующие соотношения:

$$P_{00} = \frac{\nu_1\nu_2}{\lambda(\lambda+\nu_1+\nu_2)+\nu_1\nu_2}$$

$$P_{10} = \frac{\lambda\nu_2(\lambda+\nu_1+\nu_2)}{(\nu_1+\nu_2)[\lambda(\lambda+\nu_1+\nu_2)+\nu_1\nu_2]}$$

$$P_{01} = \frac{\lambda\nu_1}{\lambda(\lambda+\nu_1+\nu_2)+\nu_1\nu_2}$$

$$P_{11} = \frac{\lambda^2\nu_1}{(\nu_1+\nu_2)[\lambda(\lambda+\nu_1+\nu_2)+\nu_1\nu_2]} \quad (4)$$

Получив соотношения, определяющие вероятности нахождения системы в состояниях A_{00}, A_{10}, A_{01}, A_{11}, мы можем выработать требования к интенсивности процессов распознания угроз для защищаемой системы и процессов их нейтрализации с учетом предполагаемой частоты проявления деструктивных факторов.

$$P_{00} = P_{INP} = \frac{\nu_1\nu_2}{\lambda(\lambda+\nu_1+\nu_2)+\nu_1\nu_2} \quad (5)$$

P_{INP} – вероятность выявления и решения проблемы, возникающей перед ЛПР.

В этом соотношении связаны три параметра.

Таким образом, была установлена аналитическая зависимость обобщённых характеристик обстановки (Δt_{PM}), информационно-аналитической деятельности (Δt_{PI}) и работ по нейтрализации деструктивных факторов (Δt_{PN}), которая может быть использована для оценки моделей информационно-аналитических систем управления процессами обеспечения информационной безопасности и получения предполагаемых значений ключевых свойств данных систем.

Результаты эксперимента

Данный метод был апробирован на примере киберфизической системы «Умный дом». Исследования показывают, что обеспечение безопасности системы «Умный дом» является одной из наиболее серьезных проблем, стоящих на пути успешного внедрения этой концепции в бытовую среду [7, 8, 9].

Одним из возможных подходов определения величин λ, υ_1 и υ_2 является использование сетевых моделей.

Сетевая модель – это графическое изображения комплекса взаимосвязанных работ, выполняемых в определенной последовательности. График состоит из элементов – работ и событий. Событие не имеет продолжительности во времени. Оно отмечает факт окончания одной или нескольких работ, определяющих возможность перехода к следующей задаче. По роли в сетевом графике различают исходное (начальное) событие – ему не предшествует ни одна работа рассматриваемого комплекса; завершающее (конечное) – после которого не производится ни одна работа, входящая в рассматриваемый комплекс; промежуточное событие, фиксирующее окончание предшествующих и начало последующих работ.

Согласно расчетам, которые были произведены при сетевом планировании, получены следующие результаты:

1) среднее время появления проблемы составляет:

Δt_{PM} = 2 (суток) =2880 (минут).

λ = 0,5 (величина обратная среднему времени проявления проблемы).

2) среднее время идентификации проблемы:

Δt_{PI} = 116 (минут) = 0,08 (суток).

ν_1 = 12,41 (величина, обратная среднему времени идентификации проблемы).

3) среднее время нейтрализации проблемы:

Δt_{PN} = 281 (минут) = 0,195 (суток).

ν_2 = 5,12 (величина, обратна среднему времени нейтрализации проблемы).

Рассмотрим условия существования процесса при заданных вероятностях:

P_{00} = 0,876

P_{10} = 0,036

P_{01} = 0,086

P_{11} = 0,016

Таким образом, мы получаем модель решения, построенную на базе синтезного подхода, позволяющую оценить свойства информационно-управляющей системы до ее построения. Данный подход позволяет обеспечить гарантированное достижение цели управления.

Выводы

В данной статье были определены типы атак на киберфизические системы, связанные с их особенностями. Установлено, что нарушение протекающих в КФС процессов и перехват контроля над ними может привести к существенному материальному ущербу и создать угрозу жизни и здоровью людей.

Для гарантированного достижения цели управления процессом обеспечения информационной безопасности КФС требуется располагать адекватной моделью информационно-управляющей системы, которая выступает в роли ЛПР.

В работе предложена методология и метод построения данной модели с использованием подхода на основе синтеза. Произведена его апробация на примере КФС «Умный дом».

Данная работа может выступать как базовое руководство при разработке моделей подсистем обеспечения безопасности КФС.

Целью дальнейших исследований является уточнение параметров модели процесса управления, в частности требуется учитывать вероятность выработки ошибочного решения, а также функционирование информационно-управляющих систем в условиях ограниченности ресурсов.

Литература

1. *Лепешкин О. М., Лепешкин М. О., Бурлов В. Г.* Синтез модели процесса управления техническими системами на основе теории радикалов. В книге: Нейрокомпьютеры и их применение. Тезисы докладов. Под редакцией А. И. Галушкина, А. В. Чечкина, Л. С. Куравского, С. Л. Артеменкова, Г. А. Юрьева, П. А. Мармалюка, А. В. Горбатова, С. Д. Кулика. 2016. С. 18-В.

2. *Burlov V. G., Popov N. N.* Management of the application of the space geoinformation system in the interests of ensuring the environmental safety of the region. В сборнике: Advances in the Astronautical Sciences. 2017. С. 751-760.

3. *Жуков А. О., Бурлов В. Г., Пестун У. А.* К вопросу стратегического планирования развития наукоемких предприятий. В сборнике: Стратегическое планирование и развитие предприятий. Материалы Восемнадцатого всероссийского симпозиума. Под редакцией Г. Б. Клейнера. 2017. С. 935-939.

4. *Анохин П. К.* Системные механизмы высшей нервной деятельности. М.: Наука. 1979. 453 с.

5. *Istomin E. P., Abramov V. M., Burlov V. G., Sokolov A. G., Fokicheva A. A.* Risk management method in parametric geosystems. В сборнике: 18th International Multidisciplinary Scientific GeoConferences SGEM 2018 Conference proceedings. 2018. С. 377-384.

6. *Бурлов В. Г., Попов Н. Н., Гарсия Эскалона Х. А.* Правление процессом применения космической геоинформационной системы в интересах обеспечения экологической безопасности региона. Ученые записки Российского государственного гидрометеорологического университета. 2018, № 50. С. 118-129.

7. *Li M., Gu W., Chen W., He Y., Wu Y., Zhang Y.* Smart Home: Architecture, Technologies and Systems, 8th International Congress of Information and Communication Technology (ICICT-2018). Vol. 131, 2018, pp. 393-400.

8. *Robles J., Kim T.* Application, systems and methods in smart home technology// A review. Int. J. Adv. Sci. Technol, 2010, pp. 37–48.

9. *Yang C., Mistretta E., Chaychian S., & Siau J.* Smart home system network architecture, 2017.

DEVELOPMENT OF CYBER-PHYSICAL SYSTEM SECURITY MANAGEMENT PROCESS MODEL

Elena S. Grozmani, *Peter the Great St. Petersburg Polytechnic University, St. Petersburg, Russia,* ***grozmani.el@yandex.ru***
Sergey V. Petrov, *Joint Stock Company "Research Institute "Rubin", St. Petersburg, Russia,* ***c.petrov13@gmail.com***

Abstract

Cyber-physical systems (CPS) combine general-purpose information and telecommunication systems and industrial networks and devices (controllers), forming a heterogeneous hierarchical distributed information technology computing environment designed for control and monitoring of technological processes. FSCs are being actively implemented in the industrial, urban and household spheres, allowing for more efficient use of resources, as well as transferring management and feedback processes to a new level. CPS are formed as a result of the aggregation of several heterogeneous information and telecommunication systems, which makes them susceptible to the destructive factors of the digital environment – cyber attacks. The peculiarities of the construction and functioning of the CPS require a new approach to defining attack surfaces and modelling threats. This is due to the fact that the "traditional" goals of attackers - the availability, integrity and confidentiality of information processed in the system - are not the only ones. In addition, the value of the information itself can be extremely low. At the same time, control and feedback processes play a decisive role in a cyber-physical system. Their stability directly affects the ability of the FSC to perform target functions, as well as the physical safety of technological facilities, personnel and consumers. Depending on the degree of criticality of the technological processes of the real world, which are controlled by the cyber-physical system, the violation of these flows inside it can lead to serious consequences, such as large material damage or a threat to the life and health of people. The severity of the identified threats is confirmed by the constantly growing number of attacks on CPS and the consequences, including potential ones, to which these attacks lead. In addition, it should be noted that in the context of the rapid development and improvement of programmable control devices (Programmable Logic Controller (PLC)), making them more accessible in the mass market segment, as well as the proliferation of high-speed wireless data transmission networks, the concept of a smart home is gaining wider application. This approach implies the integration of PLCs that interact with each other and the control centre via multi-service broadband wireless networks into the domestic environment. Thus, the concept of a smart home is based on the implementation of FSCs in places of permanent residence of people with the transfer of automatic control functions of climatic equipment, lighting, household appliances, physical elements of protection against intrusions to them. At the same time, it is extremely important to ensure the information security of the CFS. To ensure the required level of their security, it is necessary to effectively solve the problems of managing the process of ensuring their information security. The article proposes an approach to the development of a model for the information security management process of a CFS operating in a smart home.

Keywords: *cyber physical systems, information security, management, model, management decision.*

References

1. O.M. Lepeshkin, M.O. Lepeshkin, V.G. Burlov (2016). Synthesis of a model of the process of control of technical systems based on the theory of radicals. In the book: Neurocomputers and Their Applications. Abstracts of reports. Edited by A. I. Galushkin, A. V. Chechkin, L. S. Kuravsky, S. L. Artemenkov, G. A. Yuriev, P. A. Marmalyuk, A. V. Gorbatov, S. D. Kulik. P. 18-B.

2. V.G. Burlov, N.N. Popov (2017). Management of the application of the space geoinformation system in the interests of ensuring the environmental safety of the region. *Advances in the Astronautical Sciences*, pp. 751-760.

3. A.O. Zhukov, V.G. Burlov, U.A. Pestun (2017). On the issue of strategic planning for the development of knowledge-intensive enterprises. In the collection: Strategic planning and enterprise development. *Materials of the Eighteenth All-Russian Symposium. Edited by G. B. Kleiner*, pp. 935-939.

4. P.K. Anokhin (1979). System mechanisms of higher nervous activity. Moscow: Science. 453 p.

5. E.P. Istomin, V.M. Abramov, V.G. Burlov, A.G. Sokolov, A.A. Fokicheva. (2018). Risk management method in parametric geosystems. *18th International Multidisciplinary Scientific GeoConferences SGEM 2018 Conference proceedings*, pp. 377-384.

6. V.G. Burlov, N.N. Popov, Kh.A. Garcia Escalona (2018). Management of the process of using the space geoinformation system in the interests of ensuring the ecological safety of the region. *Scientific notes of the Russian State Hydrometeorological University*. No. 50, pp. 118-129.

7. M. Li, W. Gu, W. Chen, Y. He, Y. Wu, Y. Zhang (2018). Smart Home: Architecture, Technologies and Systems, *8th International Congress of Information and Communication Technology (ICICT-2018),* vol. 131, pp. 393-400.

8. J. Robles, T. Kim (2010). Application, systems and methods in smart home technology. A review. *Int. J. Adv. Sci. Technol*, 2010, pp. 37-48.

9. C. Yang, E. Mistretta, S. Chaychian & J. Siau (2017). Smart home system network architecture.

Information about authors:

Elena S. Grozmani, *Peter the Great St. Petersburg Polytechnic University, postgraduate student, St. Petersburg, Russia*

Sergey V. Petrov, *Joint Stock Company "Research Institute "Rubin", Head of Certification Testing Department, St. Petersburg, Russia*