АВТОМАТИЗАЦИЯ ПРОЦЕССА АНАЛИЗА УГРОЗ ИНФОРМАЦИОННОЙ БЕЗОПАСНОСТИ В КИБЕРФИЗИЧЕСКИХ СИСТЕМАХ

Басан Е.С.[1], Грицынин А.С.[2], Шулика М.Г.[3], Крючков В.С.[4]

Цель: *разработка методологии для автоматизации процесса анализа угроз информационной безопасности в киберфизических системах, которая основана на исследовании и анализе архитектуры системы и возможных рисков реализации угрозы, а также возможностей нарушителя.*

Метод: *разрабатываемая методология основывается на структурировании информации об архитектурных особенностях киберфизических систем. Структурирование информации и представление ее в виде каталогов, которые связаны между собой, позволяет определять по структурно-функциональной характеристике перечень актуальных для нее угроз, уязвимостей и атак. При проектировании базы данных применен онтологический подход, который позволяет выделять концепты и их свойства.*

Результаты: *разработаны методические рекомендации по анализу защищенности киберфизических систем, основанные на исследовании и оценке уязвимостей и угроз безопасности. Проведен анализ структурно-функциональных характеристики киберфизической системы и выделены основные особенности с точки зрения информационной безопасности; интегрирование новых методик по оценке рисков, определению актуальных угроз и выработке эффективных рекомендаций для киберфизических систем позволило создать базу знаний об угрозах, атаках уязвимостях киберфизических систем. Определены новые угрозы для киберфизических систем, которые связаны с их специфическими свойствами: мобильность, использование беспроводных сетей, локация вне контролируемой зоны. Итогом исследования является продукт, представленный в виде базы знаний, который позволяет определять степень опасности угрозы для заданной структурно-функциональной характеристики киберфизической системы. Реализовано автоматическое обновление информации об уязвимостях из открытых баз данных.*

Ключевые слова: *методика, атаки, инструменты атак, структурно-функциональные характеристики, база угроз, онтология, концепты, риски, ущерб.*

DOI:10.21681/2311-3456-2021-4-35-47

Введение

Проблемы стандартизации информации об угрозах в случае киберфизических систем (КФС), а также попытки определения мер по минимизации рисков является актуальной проблемой и рассматривается, как Российским, так и мировым сообществом. В случае киберфизических систем процесс определения и минимизации рисков информационной безопасности связан со следующими проблемами:

- Отсутствие актуального и принятого в Российской Федерации законодательства в области обеспечения безопасности для КФС.
- Отсутствие актуальных баз данных угроз для КФС.
- Отсутствие стандартизованного описания структурно-функциональных характеристик КФС.
- Отсутствие механизмов, средств или программных решений для автоматизации процесса определения рисков информационной безопасности и выбора требований по защите КФС. Это приводит к необходимости экспертной оценки, которая требует больших трудозатрат и является субъективной (некоторые факторы оцениваются экспертом на основе его личного опыта и мнения), что приводит к ошибкам при определении рисков, а это, в свою очередь, ведет к неадекватному выбору мер по защите. При этом возможны высокие трудозатраты и неумышленные) ошибки эксперта при оценке рисков и минимизации рисков, так как данный процесс практически полностью реализуется экспертом (имеет место так называемый человеческий фактор) и трудно поддается автоматизации [3].
- В некоторых случаях эксперты умышленно занижают риски и исключают угрозы, от которых сложно и «дорого» защищаться, для того чтобы сэкономить сред-

1 Басан Елена Сергеевна, кандидат технических наук, доцент кафедры Безопасности информационных технологий Института компьютерных технологий и информационной безопасности Южного Федерального Университета «ЮФУ», г. Таганрог, Россия. E-mail: ebasan@sfedu.ru, ORCID 0000-0001-6127-4484.

2 Грицынин Антон Сергеевич, студент кафедры Безопасности информационных технологий Института компьютерных технологий и информационной безопасности Южного Федерального Университета «ЮФУ», г. Таганрог, Россия. E-mail: anton97_07@mail.ru

3 Шулика Мария Геннадьевна, студентка кафедры Безопасности информационных технологий Института компьютерных технологий и информационной безопасности Южного Федерального Университета «ЮФУ», г. Таганрог, Россия. E-mail: mshulika@sfedu.ru

4 Крючков Василий Сергеевич, ассистент кафедры Безопасности информационных технологий Института компьютерных технологий и информационной безопасности Южного Федерального Университета «ЮФУ», г. Таганрог, Россия. E-mail: kryuchkov@sfedu.ru

ства оператора на закупку средств защиты. Либо, наоборот, эксперт может умышленно увеличивать затраты на закупку средств защиты.

Авторами работы [1] делается попытка выделить большинство известных угроз на разных уровнях архитектуры «Интернет вещей» (IoT) с акцентом на возможность реализации атак, используя вредоносные программы. Авторы представляют развернутую методологию реализации атак на IoT, а также подробный сценарий распределенной атаки типа «отказ в обслуживании» через ботнет IoT с последующими необходимыми мерами повышения информационной безопасности. Авторы предлагают руководство по разработке методологии обеспечения безопасности IoT, основанной на лучших зарубежных отраслевых практиках. Методология включает в себя оценку рисков, средства безопасности, повышающие конфиденциальность, целостность и доступность информации, а также метод расчета воздействия выявленных рисков [4]. Тем не менее, представленной информацией может воспользоваться только эксперт для самостоятельной оценки рисков, угроз и выбора мер по защите, и эта работа потребует большого количества его времени и внимания. Отсутствие автоматизации процесса в данном случае является серьезным недостатком. Кроме того, при оценке рисков не учитываются риски, связанные с объектом, которым «управляет» «Интернет вещей» [5].

National Institute of Standards and Technology (NIST) представил стандарт «Framework for Improving Critical Infrastructure Cybersecurity» – Стандарт для повышения кибербезопасности критических информационных систем [6]. Документ состоит из трех частей: ядро стандарта, уровни реализации и профили стандарта. Базовое ядро платформы представляет собой набор мероприятий, результатов и информационных справочников по кибербезопасности, которые являются общими для секторов и критически важной инфраструктуры. Элементы Ядра предоставляют собой подробное руководство по разработке индивидуальных организационных профилей. Уровни предоставляют организациям механизм для просмотра и понимания характеристик их подхода к управлению рисками кибербезопасности, что поможет в определении приоритетов и достижении целей кибербезопасности [7].

В Российском законодательстве наиболее близким методическим документом, который описывает требования по информационной безопасности для автоматизированных систем управления технологическим процессом (АСУ ТП), является: Приказ Федеральной службы по техническому и экспортному контролю от 14 марта 2014 г. N 31 «Об утверждении Требований к обеспечению защиты информации в автоматизированных системах управления производственными и технологическими процессами на критически важных объектах, потенциально опасных объектах, а также объектах, представляющих повышенную опасность для жизни и здоровья людей и для окружающей природной среды» [8]. Этот документ рассматривает вопросы структурирования АСУ ТП, а также предлагает различные подсистемы безопасности. В документе не учитывается, что исполнительные механизмы (которые могут включать в себя сенсорные узлы, актуаторы) сами по себе могут автономно управлять решениями или действовать в отдельной группе. В то же время посредники между группой исполняющих устройств и оператором (устройства на уровне автоматического управления) часто могут отсутствовать, когда речь идет о полностью распределенной системе [9]. Технологический процесс в качестве объекта защиты не учитывается, хотя за счет кибератаки или другого негативного процесса путем воздействия на компоненты информационной системы может быть оказано негативное влияние непосредственно на технологический процесс [10].

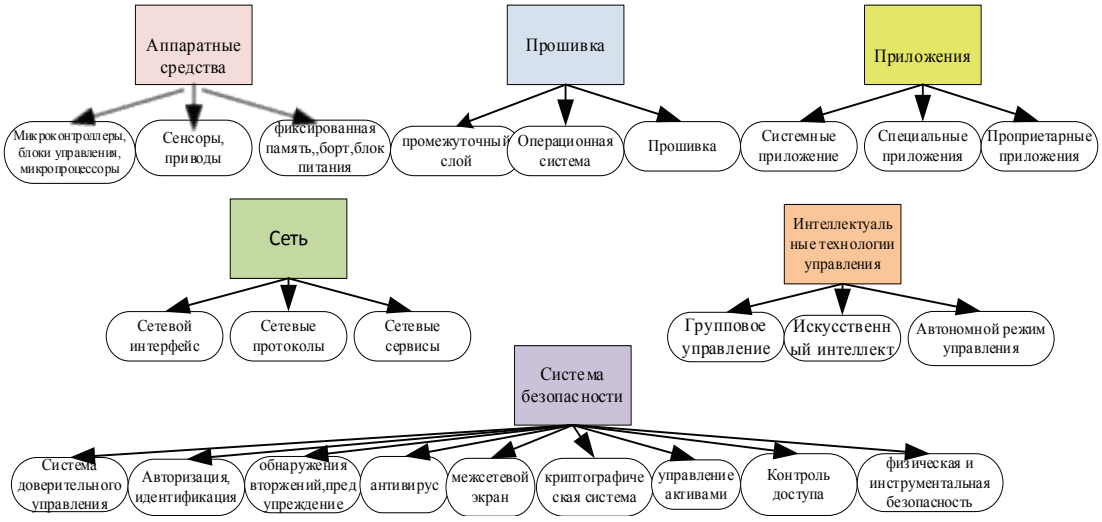

Рис. 1. Компоненты киберфизической системы

1. Анализ архитектуры киберфизических систем

КФС является многосоставной и может включать в себя тысячи различных датчиков и сенсоров, которые обмениваются между собой информацией, аккумулируют ее и передают на управляющее устройство [11]. На рисунке 1 показана схема структурно–функциональных характеристик КФС, которая выявляет новые аспекты в архитектуре КФС и позволяет более точно определить те или иные угрозы, которые могут быть реализованы на КФС, в том числе в данном исследовании выделен компонент интеллектуального управления [12,13].

Важно понимать то, что каждый из представленных элементов системы имеет собственные уязвимости, которые может проэксплуатировать злоумышленник. Также важным компонентом являются интеллектуальные технологии, которые могут быть подвергнуты новым типам уязвимостей. На пример, на сегодняшний день становится актуальной проблема анализа валидности и подлинности данных для обучений нейронных сетей. Это связано с тем, что генерация новых данных – трудоемкий процесс и зачастую данные берутся из открытых источников. При этом злоумышленник может подменить данные для обучения и сеть будет обучена неверно, соответственно будет принимать не правильные решения.

КФС являются новой областью исследования, поскольку в отличии от привычных компьютерных и информационных систем КФС обладает рядом особенностей [14]:

1. КФС имеет смешанную структуру, состоящую не только из информационных аспектов, осуществляющих управление технологическими процессами, но и физическими компонентами.

2. КФС имеет коммуникационную среду, в которой происходит непрерывный обмен большими массивами данных внутри системы и за ее пределами.

3. Компоненты КФС могут быть мобильными и располагаться вне контролируемой зоны.

4. КФС зависит от информации, от внешних информационных воздействий, направленных на подсистему управления, на интерфейс взаимодействия оператора с системой, на устройства, которые являются частью КФС, на протоколы взаимодействия и сетевое оборудование.

5. Такими системами можно управлять как путем изменения параметров, так и путем изменения структуры КФС с перераспределением функций между компонентами.

6. КФС часто являются гетерогенными системами, которые сочетают в себе большое количество разных технологий.

В типовых информационных системах (ИС) атрибутами безопасности являются конфиденциальность, целостность и доступность информации

В данной работе атрибутами безопасности будут являться структурно- функциональные характеристики, приведенные на рис. 1.

2. Разработка методики обеспечения безопасности КФС

Методика включает в себя несколько уровней вычислений для того, чтобы определить в конечном счете актуальность той или иной угрозы. Идея заключается в том, что владелец КФС передает в систему информацию о структурно-функциональных характеристиках и в итоге получает список актуальных угроз и рекомендаций для КФС.

2.1. Уровень критичности

Методика устанавливает уровень критичности компонентов киберфизических систем. Уровень критичности определяется потенциальным ущербом для подсистемы, в отношении которой производятся действия, ставящие под угрозу безопасность информации и модулей киберфизической системы, необходимых системе для достижения поставленных задач. Защита модулей системы, выполнение ими поставленных задач, поддержания на должном уровне функций является важной задачей.

У каждого атрибута есть подсистемы, которые и будут являться оценочными. Под понятием подсистема понимаются СФХ входящие в тот или иной атрибут. Предлагается три уровня критичности высокий, низкий и средний, которые зависят от последствий проведенной атаки на ту или иную подсистему. Под уровнем критичности понимается то, какие последствия потерпит система при реализации угрозы на тот или иной атрибут КФС [15]. Распределение уровней критичности для каждой подсистемы представлены в таблице 1.

Ценность подсистемы оценивается от низкой до высокой. Уровни критичности присваивались исходя из важности систем и подсистем, а также количества угроз, которые возможны на той или иной подсистеме и считались по формуле (1):

$$C = T + I, \quad (1)$$

где C – уровень критичности; T – количество угроз, реализуемых на ту или иную подсистему; I – важность подсистемы.

2.2. Анализ уровня гетерогенности системы

При определении угроз безопасности информации на этапе создания КФС в случае, когда меры защиты информации не реализованы или не проведена оценка их достаточности и эффективности, необходима оценка возможности реализации угрозы. Данная оценка характеризуется, вероятностью реализация той или иной угрозы безопасности информации в КФС с заданными структурно-функциональными характеристиками и особенностями функционирования, которая проводится относительно уровня проектной защищенности КФС [16].

Под уровнем проектной защищенности понимается исходная защищенность КФС, обусловленная заданными при проектировании структурно- функциональными характеристиками и условиями ее функционирования. Уровень проектной защищенности определяется на основе анализа проектных структурно-функциональных характеристик, представленных в таблице 2 [17].

Уровень начальной защищенности информационной системы рассчитывается из степени гетерогенности и количества набранных баллов по уровню проектной защищенности КФС, рассчитывается это по формуле (2).

DOI:10.21681/2311-3456-2021-4-35-47

Таблица 1

Ценность подсистем

Тип структурно-функциональной характеристики	Ценность подсистемы		
	Низкий	Средний	Высокий
Аппаратное обеспечение. • Микроконтроллеры, микропроцессоры. • Сенсоры, актуаторы. • Память, аккумулятор, другие вспомогательные блоки, шины данных.		 +	 + +
Микропрограммное обеспечение: • Микропрограммные средства. • Операционная система. • Драйвера.	 +	 + +	
Программные средства • Системные программы (встроенные). • Специальные приложения (разработанные для задач киберфизической системы). • Пользовательские приложения.	 +	+ +	
Сетевое обеспечение • Сетевые интерфейсы. • Сетевые протоколы. • Сетевые сервисы.		+ + +	
Интеллектуальные технологии управления: • Групповое управление. • Искусственный интеллект. • Автономной режим управления.			
Система безопасности: • Система доверительного управления. • Авторизация, идентификация. • Обнаружение вторжений. • Антивирус. • Межсетевой экран. • Криптографическая система. • Управление активами. • Контроль доступа. • Физическая и инструментальная безопасность.	 + +	 + + + + + + +	 +

Таблица 2

Показатели, характеризующие проектную защищенность информационной системы

Структурно-функциональные характеристики информационной системы, условия ее эксплуатации	Уровень проектной защищенности КФС		
	Высокий	Средний	Низкий
По наличию (отсутствию) взаимосвязей с иными информационными системами: • взаимодействующая с системами, • невзаимодействующая с системами.		 +	 +

Структурно-функциональные характеристики информационной системы, условия ее эксплуатации	Уровень проектной защищенности КФС		
	Высокий	Средний	Низкий
По наличию (отсутствию) взаимосвязей (подключений) к сетям связи общего пользования: • подключенная, • подключенная через выделенную инфраструктуру (gov.ru или иную), • неподключенная.	 +	 +	 +
По размещению технических средств: расположенные в пределах одной контролируемой зоны, расположенные в пределах нескольких контролируемых зон, – расположенные вне контролируемой зоны.	 +	 +	 +
По степени мобильности: • стационарные, • мобильные.		 +	 +
По способу управления: • операторское управление, • полуавтоматическое управление, • автономное управление, • групповое управление.		 + +	 + +
По условиям функционирования: • детерминированные (определенные) среды, • недетерминированные (неопределенные).		 +	 +
По областям применения: • промышленные, • бытовые, • социальные, • медицинские, • исследовательские, • боевые.		 + + +	 + + +
По среде функционирования: • космические, • воздушные, • наземные, • подземные, • морские.	 +	 + +	 + +
По условиям функционирования: • детерминированные (определенные) среды, • недетерминированные (неопределенные).		 +	 +
По типу топологии сети • звезда, • ad-hoc сеть, • mesh сеть.		 + +	 +

$$P = S + G, \quad (2)$$

где P – уровень начальной защищённости системы; G – количество набранных баллов на проектной защищенности информационной системы; S – степень гетерогенности сети, рассчитывается по формуле. S рассчитывается по формуле (3):

$$S = \frac{Q * R}{100} \quad (3)$$

где Q – является константой; R – зависит от уровня гетерогенности.

2.3. Степень сложности реализации атаки

Инструменты для проведения этаки — это программные или программно-аппаратные средства, которые будет использовать злоумышленник для реализации той или иной атаки (A):

- Атака реализуется стандартными программными средствами, доступными в Интернете, которые не требуют дополнительной доработки и использования навыков.
- Атака осуществляется стандартным программным обеспечением, доступным в Интернете, требующим дополнительной доработки и специальных навыков использования.
- Атака реализуется с помощью программного и аппаратного обеспечения, доступного на потребительском рынке для покупки, не требующего дополнительной доработки, и навыков использования.
- Атака реализуется программным и аппаратным обеспечением, доступным для покупки на потребительском рынке, при этом требуются дополнительные усовершенствования и специальные навыки использования.
- Атака осуществляется с использованием специально разработанных программных средств.
- Комплексное воздействие на объект атаки с использованием методов социальной инженерии, психологии и т. д.
- Атака осуществляется с использованием специально разработанного программного и аппаратного обеспечения.

Способ реализации атаки – это сценарий, который определяет вектор атаки и точку входа в систему (W):

- Атака осуществляется с помощью удаленного доступа.
- Атака осуществляется через прямой физический доступ.
- Атака осуществляется путем непосредственного воздействия на структурные и функциональные характеристики.
- Атака осуществляется путем косвенного воздействия на структурные и функциональные характеристики (влияние на параметры окружающей среды и т. д.).
- Атака осуществляется путем воздействия на одну структурно-функциональную характеристику через другую структурно-функциональную характеристику (многоступенчатая атака).
- Атака осуществляется путем воздействия на персонал управляющий КФС.

Сложность реализации атаки рассчитывается по формуле (4):

$$H = W * A, \quad (4)$$

где H – Сложность реализации атаки; W – Способ реализации атаки; A – инструменты для проведения атаки.

Далее необходимо определить, какие последствия могут возникнуть в результате проведения конкретной атаки. Для каждого типа ущерба определяются три степени: низкий, средний, высокий. Тип ущерба имеет обозначения D и представлен в таблице 3.

Таблица 3

Степень и тип ущерба

Тип ущерба	Степень ущерба		
	Низкая	Средняя	Высокая
Экономический			+
Социальный	+		
Политический		+	
Репутационный	+		
Техногенный	+		
В области обороны			+
Безопасности государства			+

Таблица 4

Уровень ценности актива

Наименование актива	Уровень ценности		
	Низкая	Средняя	Высокая
информация			
программно-аппаратные средства			
программные средства;			
средства защиты информации;			
обеспечивающие системы;			
сущность, продукт			

2.4. Определение ценности информационного ресурса

Ущерб может быть оценен с учетом стоимости активов, которыми обладает владелец системы [9-10]. В данной методике выделены следующие активы: информация, программно-аппаратные средства, программные средства, средства защиты информации, конечный производимый продукт или объект, которым управляет КФС. Предлагается добавить к стандартному набору ресурсов объект, которым управляет КФС, или продукт, являющийся результатом работы. Добавление этой сущности важно, потому что злоумышленник может, воздействовать на параметры окружающей среды и изменить показания КФС, что в итоге может привести к неправильным действиям оператора или искусственного интеллекта. И наоборот, результаты атаки могут повлиять на КФС, которая анализирует среду, злоумышленник может подделать данные или заблокировать сеть. Оценка ценности активов представлена в таблице 4:

Для каждого актива также определяются три уровня стоимости: высокий, средний, низкий. Эта характеристика должна быть оценена владельцем системы.

2.5. Степень опасности реализации угроз на СФХ

Чтобы определить какой ущерб нанесет та или иная угроза, реализованная на одну из перечисленных выше СФХ, применим формулу (5).

$$M = H + P + C + D + L, \quad (5)$$

где M – степень опасности реализации угрозы.

Предлагается три показателя для определения степени опасности реализации угрозы (низкая степень, средняя и высокая). Данная оценка характеризуется масштабностью тех потерь, которые могут возникнуть при реализации угрозы. Этот показатель является комплексным и учитывает все предыдущие вычисления.

3. Разработка базы данных угроз киберфизической системы

3.1. Разработка архитектуры базы данных

Увеличение количества угроз информационной безопасности, связанное с ростом числа производителей, устройств, информационных технологий и количества КФС, требует создания и постоянного обновления базы знаний об угрозах, уязвимостях и требованиях по безопасности КФС, в таком исполнении, которое позволило бы упростить процесс интегрирования баз знаний с экспертными системами, искусственным интеллектом, а также решило бы проблему построения взаимосвязей между различными сущностями баз знаний и процедуру их обновления. Предлагается разработка модели организации базы знаний в области информационной безопасности КФС на основе онтологических моделей представления знаний. Ядром базы знаний является концептуальная модель в области безопасности информационных систем, которая будет включать такие типовые концепты в области безопасности, как «угроза», «уязвимость», «требование безопасности», «атака», «рекомендация», которые предполагается дополнить концептами КФС, а также установить отношения между концептами (например, отношение «подмножество» между концептами «атака» и «угроза», атака – это преднамеренная угроза). Научная значимость заключается в двух моментах. Первое – в мировой литературе предлагаются различные варианты моделей представления знаний для концептов предметной области безопасности информационных систем, однако отсутствует интегрированная модель, связывающая всевозможные концепты и их модели. Вторым новым аспектом предлагаемого подхода является учет специфики КФС в интегрированной модели представления знаний.

Основными концептами являются уязвимости, атаки, угрозы, нарушители, структурно-функциональные характеристики и требования, связанные между собой следующим образом:

DOI:10.21681/2311-3456-2021-4-35-47

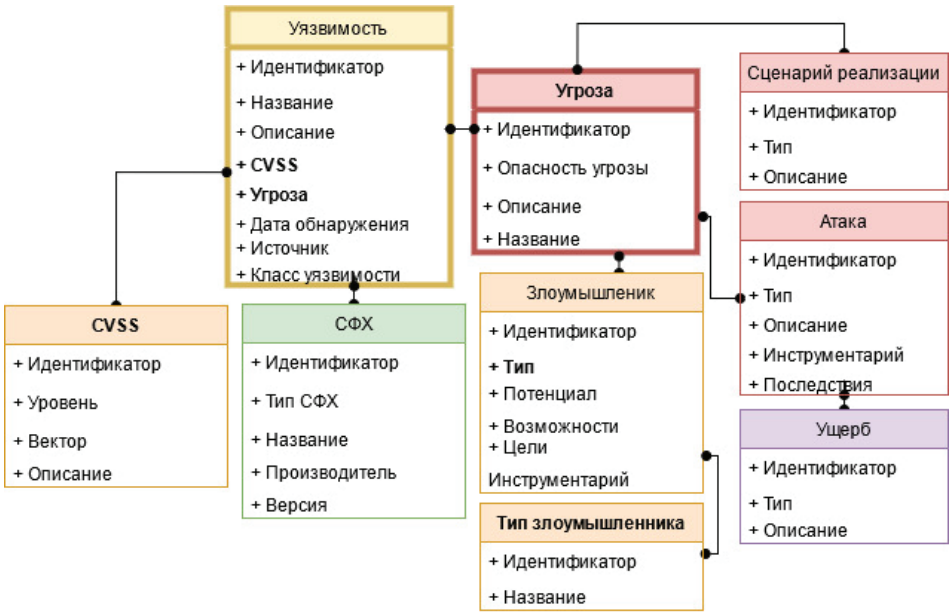

Рис.2. Структурная схема базы данных, часть с угрозой

— угроза связана с уязвимостью, как многие к одному;
— угроза и атака имеют связь многие ко многим;
— угроза и нарушитель имеют связь многие ко многим;
— угроза и структурно-функциональные характеристики имеют связь многие ко многим;
— угроза и требования имеют связь многие ко многим.

Остальные сущности являются вспомогательными и расширяют описания основных концептов. Структура всей базы представлена на рис. 2.

Данный рисунок отражают связи между концептами базы данных. Центральными объектами являются каталоги угроз и уязвимостей, они связаны с большим количеством концептов.

Уязвимость связана со структурно-функциональной характеристикой, как многие ко многим, потому что одна уязвимость может существовать в разных ПО, также у одного ПО может быть несколько уязвимостей.

Концепты, описывающие угрозы и злоумышленника, детализированы с использованием дополнительных каталогов: CVSS для угроз и тип нарушителя, которые используются для более детального описания концептов.

Также уязвимость связана с угрозой, как один ко многим, потому что уязвимость даёт возможность выявить единственную угрозу.

После проведения атаки организации несут ущерб в разных областях, поэтому связь между этими моделями многие ко многим.

Несколько угроз можно использовать для проведения одной атаки, также несколько атак могут использовать одну угрозу, поэтому их связь многие ко многим.

Разные требования или совокупность требований можно применить по устранению угрозы, также некоторые требования повторяются, поэтому у нескольких угроз, может быть, одинаковые требование по устранению.

Концепты нарушителя и последствия реализации угрозы также имеют связь многие ко многим с моделью угрозы для более детального описания.

Одной из ключевых особенностей является возможность обновления информации об угрозах путем интеграции с внешними банками данных. Скрипт с определенной периодичностью, например один раз в день, загружает с внешней базы актуальный перечень уязвимостей. Список фильтруется по заданным параметрам, чтобы отобрать только интересующие уязвимости, например по списку имен или статусу, и переводится в json формат, для последующей удобной записи во внутреннюю базу данных.

3.2. Пример угроз из каталога

Угроза применения методов обратного инжиниринга для получения информации о типе загрузчика, контроллера полетов и протокола загрузчика

- Описание угрозы: угроза состоит в возможности получения злоумышленником информации о типе протокола загрузчика за счет того, что многие протоколы являются открытыми. Протоколы загрузчиков либо определяются производителями микросхем, либо документируются сообществом разработчиков. Кроме того, протоколы могут быть инвертированы путем просмотра последовательной связи с использованием любого из анализаторов последовательного порта, такого как PortMon от Sysinternals или Serial Port Monitor. Для анализа протокола также можно посмотреть исходные файлы загрузчика, доступные в проектах с открытым исходным кодом.
- Объект воздействия: протоколы, сетевой трафик, платы управления.
- Последствия угрозы: подмена аппаратного обеспечения и перепрошивка узла КФС позволяют внедрить злоумышленнику «своего» агента в систему группового управления. И далее злоумышленник сможет производить различные атаки на сеть. Данная атака может привести к потере управлением КФС. При

этом злоумышленник имеет возможность получить в пользование КФС.

На каком уровне СФХ реализуется угроза: сеть, протоколы связи.

Угроза высокого напряжения на плате управления

- Описание угрозы: подача высокого напряжения приведет в неработоспособное состояние КФС.
- Объект воздействия: пульты управления БПЛА.
- Последствия угрозы: повреждения модуля КФС, на котором была реализована угроза.
- На каком уровне СФХ реализуется угроза: аппаратное обеспечение.

Угроза удаленного потребления ресурсов

- Описание угрозы: угроза заключается в том, что злоумышленник может оказывать влияние на потребляемые узлами КФС энергетические ресурсы (т.е. на количество расходуемой энергии в единицу времени) путем постоянной отправки им пакетов, а, также, не давая узлу КФС уйти в спящий режим. Кроме того, злоумышленник может воздействовать на пропускную способность сети, затопляя сеть пакетами. Также злоумышленник может инициировать процедуру деаутентификации, что задействует дополнительное расходование энергетических ресурсов. Помимо сетевого воздействия злоумышленник может оказывать физическое воздействие на ресурсы узлов сети.
- Объект воздействия: плата управления узла КФС, датчики.
- Последствия угрозы: нарушение свойства конфиденциальности передаваемой информации. Нарушение свойства доступности передаваемой информации, а также доступности узлов сети.
- На каком уровне СФХ реализуется угроза: сеть.

Угроза изменения компонентов системы

- Описание угрозы: угроза заключается в возможности получения нарушителем доступа к сети Интернет (при его отсутствии в системе), к хранимым на личных мобильных устройствах файлах, внедрение закладок и т.п. путём несанкционированного изменения состава программных или аппаратных средств информационной системы, что в дальнейшем позволит осуществлять данному нарушителю (или другому – внешнему, обнаружившему несанкционированный канал доступа в систему) несанкционированные действия в данной системе. Данная угроза обусловлена слабостями мер контроля за целостностью аппаратной конфигурации информационной системы. Реализация данной угрозы возможна при условии успешного получения нарушителем необходимых полномочий в системе.
- Объект воздействия: системное программное обеспечение, прикладное программное обеспечение, сетевое программное обеспечение.
- Последствия угрозы: частичная дестабилизация работы сети за счёт вывода из строя одного или нескольких мобильных устройств.
- На каком уровне СФХ реализуется угроза: операционная системы, программное обеспечение.

Угроза несанкционированного доступа к программно-аппаратному обеспечению узлов КФС за счет их расположения вне контролируемой зоны

- Описание угрозы: узлы КФС могут располагаться в незащищенных и неконтролируемых средах, при этом злоумышленник может достаточно легко перехватить любой узел КФС в свое пользование. Как правило, программное обеспечение КФС строится на основе линукс подобных операционных систем, причем количество существующих типов как самих микроконтроллеров или бортовых вычислителей, так и программного обеспечения для них является ограниченным. Таким образом, злоумышленник, обладающий знаниями об особенностях устройства таких систем, сможет внедрить собственный код и изменить конфигурацию системы. Кроме того, злоумышленник сможет поменять аппаратную конфигурацию устройства, изменив конфигурацию сенсоров, а также элемент питания узла КФС.
- Объект воздействия: прикладное программное обеспечение, системное программное обеспечение.
- Последствия угрозы: частичная дестабилизация работы сети за счёт вывода из строя одного или нескольких устройств. Внедрение злоумышленника на данном этапе может привести к нарушению возможности функционирования узлов КФС, а также к нарушению процесса выполнения целей отдельным узлом КФС или группой узлов. Нанесение деструктивного воздействия на сеть, и частичный отказ работы системы.
- На каком уровне СФХ реализуется угроза: программно-аппаратное обеспечение.

Угроза получения сведений о владельце беспроводного устройства

- Описание угрозы: угроза заключается в возможности раскрытия нарушителем сведений о географических перемещениях дискредитируемого пользователя в определённые промежутки времени, в том числе выявить место его работы, проживания и т.п. Получение таких сведений может использоваться нарушителем в дальнейшем для реализации угроз в информационных системах, доступ к которым имеет дискредитируемый пользователь. Данная угроза обусловлена слабостью защиты идентификационной информации беспроводных точек доступа при их подключении к сети Интернет. Реализация данной угрозы возможна при условии наличия у нарушителя доступа к идентификационными данным стационарных точек беспроводного доступа, с которыми в автоматическом режиме осуществляет взаимодействие беспроводное устройство дискредитируемого пользователя.
- Объект воздействия: сетевой узел, метаданные.
- Последствия угрозы: нарушение конфиденциальности.
- На каком уровне СФХ реализуется угроза: протоколы связи, сеть.

Угроза воздействия злоумышленника на параметры окружающей среды

- Описание угрозы: злоумышленник может создать физические препятствия для КФС, чтобы помешать выполнить заданную цель. Эти препятствия зависят от

набора действий, которые доступны КФС. Если узлы КФС сконфигурированы для доставки товара к определенной цели, то атакующий может последовать за ними, мешая достичь цели, кроме того, атакующий может использовать более мощный приемопередатчик, чтобы заглушить канал связи.
- Объект воздействия: сенсорная система, отвечающая за движение и ориентацию в пространстве узла КФС.
- Последствия угрозы: провал поставленной задачи, уничтожение узла КФС.

Угроза электромагнитного воздействия на узлы КФС
- Описание угрозы: принцип электромагнитного воздействия заключается в появлении наведенных токов на антеннах узла КФС. Угрозу электромагнитных воздействий можно разделить на 2 типа: естественного (природного) происхождения и искусственного происхождения. Естественные угрозы включают в себя прямой удар молнии, электромагнитное поле близкого удара молнии. Искусственное происхождение включает в себя боевые электромагнитные воздействия (ЭМВ) (воздействия средств поражения), реализующиеся только в боевой обстановке. ЭМВ техногенного происхождения.
- Объект воздействия: паразитные антенны (проводники на печатной плате, многочисленные проводники, входящие в состав аппаратуры, межблочные соединительные кабели).
- Последствия угрозы: воздействие наведенных токов на паразитные антенны, может привести к отказам работы электронного оборудования бортовой системы управления и отказам катастрофической степени.
- На каком уровне СФХ реализуется угроза: аппаратная часть.

Угроза обнаружения по электромагнитным наводкам
- Описание угрозы: обнаружения по электромагнитным наводкам возникает при излучении информационных сигналов различными элементами технических средств узлов КФС или при наличии гальванических связей со средствами вычислительной техники. Просачивание информационных сигналов в сети электропитания возможно при наличии реакции выпрямителя на работу устройств с информационными сигналами. В основном источником электромагинтной наводки являются накопители на жёстком и гибком дисках (включая внешние ZIP, JAZ), устройства CD и DVD, устройства внешней «Флэш» памяти, клавиатура, последовательный порт (COM), последовательный порт (USB), принтеры, видеоподсистемы. Обнаружение каких-либо наводок производится различными программно-аппаратными комплексами или системами, в которых установлены различные приемники и антенны, которые могут перехватывать видеосигнал, представляющий собой чередование прямоугольных импульсов на приборе. Каждая строка растра при этом представляет собой пакет импульсов. Путем такого перехвата возможна утечка данных.
- Объект воздействия: аппаратная часть.
- Последствия угрозы: обнаружение по электромагнитным наводкам может привести к тому, что узел КФС выдаст свое местоположение в радиусе обхвата антенн какой-либо системы или аппаратно-программного комплекса, а приемник, который установлен на этих комплексах и системах, может привести к перехвату видеосигнала или секретной информации в виде пакета импульсов.
- На каком уровне СФХ реализуется угроза: аппаратная часть.

Угроза зашумления сигнала на частоте 960 МГц
- Описание угрозы: принцип зашумления сигнала имеет три типа работ:

1) специальные подавляющие устройства («глушилки») излучают сигнал в том же диапазоне частот, что и устройство, которое требуется подавить. Вокруг глушилки создается поле «белого шума», в котором теряются сигналы от других источников;

2) создается электромагнитный экран, не позволяющий проходить ни входящим, ни исходящим сигналам;

3) на телефон или шпионскую аппаратуру отправляется сигнал, временно выводящий оборудование из рабочего состояния.

Устройства глушения подразделяются на портативные и стационарные.

Портативные отличаются очень небольшими размерами и весом. Эффективное покрытие – до 15 метров. При необходимости прибор размещается в машине, портфеле, комнате переговоров. Эффективны, если необходимо заглушить сигналы CDMA, 3G, Wi-fi, GSM, DCS, GPS.

Стационарные – радиус действия увеличивается до 40 метров, в том числе на открытом пространстве. С помощью подобного оборудования можно обеспечить тишину и конфиденциальность во время совещания, на встрече с партнерами, во время спектакля или иного массового мероприятия. Антенны обеспечат подавление сигналов CDMA, GSM, DCS, PHS, PCS, 3G (WCDMA), Wi-Fi, 4G LTE.

На частотах 960 МГц в основном используют скрытые GSM-камеры, GSM-жучки, а также мобильную связь GSM900. Установив подавитель сигнала на данную частоту данные устройства выйдут из строя.
- Объект воздействия: GSM-устройства
- Последствия угрозы: зашумление на частотах 960 МГц введет к сбою работы GSM-устройств. Если необходимо использовать GSM-камеру или жучок, то в этом случае будет гарантия, что GSM камеры окажутся бесполезны, а тот, кто их установил, не получит ценную информацию.

Заключение

В заключении следует отметить, что данная работа носит важный характер для обеспечения ИБ в КФС [19]. Основной целью данной работы являлась разработка методики для анализа угроз информационной безопасности в киберфизических системах. Для достижения поставленной цели были решены следующие задачи:
- проведена систематизация данных о киберфизических системах;
- проведен анализ структурно–функциональных характеристик киберфизических систем;

- проведен анализ внешних и внутренних атак на киберфизических систем;
- разработана методика анализа защищенности для киберфизических систем;
- реализована база знаний об угрозах КФС.

Авторы провели анализ структурно-функциональных характеристик киберфизических систем и структурировали их, затем определили набор факторов, которые влияют на их защищённость и определили уровень исходной защищенности исходя из наличия тех или иных факторов [20].

На сегодняшний день методики определения вероятного нарушителя оценивают его с точки зрения целей и возможностей [21,22]. При этом, если речь идет о КФС, то нарушитель, обладающий низким потенциалом, то есть возможностями использовать стандартные и общедоступные утилиты для проведения атак, может нанести значительный ущерб объекту, который находится под управлением КФС. Поэтому целесообразно при рассмотрении нарушителя учитывать не только его воздействие на информацию и на технические средства, но и на объект, который находится под наблюдением или управлением КФС. Такая концепция предполагает необходимость пересмотра модели вероятного нарушителя и разработки методики его определения. Определение целей и возможностей нарушителя также проводится экспертным путем, и чёткие рекомендации практически отсутствуют. В методике ФСТЭК представлен широкий круг нарушителей, но какие из них являются вероятными для данной системы, определяет эксперт на основе собственных умозаключений. Новизна предлагаемой методики заключается в разработке набора факторов, определяющих ветряного нарушителя для КФС. В частности, отдельно рассматриваются атаки и инструменты атак, которыми может воспользоваться нарушитель [23].

Итоговым продуктом является база знаний об угрозах и уязвимостях КФС. За счет того, что база знаний построена на основе онтологической модели, она позволяет атрибутировать угрозы, атаки, уязвимости, СФХ и устанавливать между ними взаимодействия.

В дальнейшем планируется развитей базы знаний об угрозах, атаках, уязвимостях до уровня информационно-аналитического ресурса, которым могли бы пользоваться владельцы и разработчики КФС. Подобный ресурс должен позволить автоматизировать процесс определения требований по безопасности для КФС и мер по минимизации рисков.

Статья подготовлена при поддержке Фонда содействия развитию инноваций. Контракт № 612ГУЦЭС8-D3 / 61995.

Литература

1. Makhdoom I., Lipman J., Ni. W. Anatomy of Threats to the Internet of Things // IEEE Communications surveys & Tutorials, vol. 21, no. 2, second quarter. 2019. Pp. 1636-1675.
2. Siboni S., Sachidananda V., Meidan Y., Bohadana M., Mathov Y., Bhairav S., Shabtai A., Elovici Y. Security Testbed for Internet-of-Things Devices. // IEEE transactions on reliability, 2019. №68 (1). Pp. 23-44.
3. Atamli A.W., Martin A. Threat-based Security Analysis for the Internet of Things. In International Workshop on Secure Internet of Things. 2014, pp. 36-43.
4. Zhou W., Yu B. A Cloud-Assisted Malware Detection and Suppression Framework for Wireless Multimedia System in IoT Based on Dynamic Differential Game // China Communications. 2018. Pp. 209-223.
5. Carielli S., Eble M., Hirsch F., Rudina E., Zahavi R. IoT Security Maturity Model // Practitioner's Guide. Version 1.0. 2019. 129 p.
6. National Institute of Standards and Technology. Framework for Improving Critical Infrastructure Cybersecurity. Version 1.1. 2018. 55 p.
7. Sarfraz A., Mohammad M. R., Chowdhury J.N. Interoperability of Security Enabled Internet of Things // Wireless PersCommun. 2011. № 61. Pp. 567-586.
8. Tao M., Zuo J., Liu Z.; Castiglione A., Palmieri F. Multi-layer cloud architectural model and ontology-based security service framework for IoT-based smart homes. Future Gener // Computer Systems. 2018. № 78. Pp. 1040-1051.
9. Ekelhart A., Fenz S., Neubauer T. AURUM: A Framework for Information Security Risk Management. In Proceedings of the 2009 42nd Hawaii International Conference on System Sciences. IEEE, 2009. Pp. 1-10.
10. Mozzaquatro B. A., Agostinho C., Goncalves D., Martins J., Jardim-Goncalves R.. An Ontology-Based Cybersecurity Framework for the Internet of Things // Sensors. 2018. № 18. Pp. 3053 -3055.
11. Abbass W., Bakraouy Z., Baina A., Bellafkih M. Classifying IoT security risks using Deep Learning algorithms. In 6th International Conference on Wireless Networks and Mobile Communications (WINCOM), 2018, pp. 1-10.
12. Fedorchenko A. V., Doynikova E. V., Kotenko I. V. Automated detection of assets and calculation of their criticality for the analysis of information system security // Tr. SPIIRAN. 2019. № 18(5). Pp. 1182-1211.
13. Electronic resource https://threatmodeler.com/ - access mode is free (Date of access 10.05.2021).
14. Bakhshi Z., Balador A., Mustafa J. Industrial IoT security threats and concerns by considering Cisco and Microsoft IoT reference models. In Wireless Communications and Networking Conference Workshops (WCNCW). IEEE, 2018, pp. 173-178.
15. Basan E., Basan A., Grutsynin A. Analysis of the Security Problems of Robotic Systems. In 2nd International Conference on Intelligent Communication and Computational Techniques (ICCT), 2019, pp. 1200-1214.
16. Electronic resource Facial Recognition Implemented at Beijing Capital International Airport – URL: https://medium.com/@pandaily/facial–recognition–implemented–atbeijing–capital– inter- national–airport–8c0b7cc1b945 (Date of access 12.03.2021).

17. Dieber B., Breiling B., Taurer S., Kacianka,S., Rass,S., Schartner P. Security for the Robot Operating System // Robot. Auton. Syst. 2017. № 98(C). Pp. 192–203.
18. National Institute of Standards and Technology, Framework for Improving Critical Infrastructure Cybersecurity, April 16, 2018, version 1.1, P.32-43.
19. Breiling, B., Dieber, B. and Schartner, P. Secure communication for the robot operating system. In Annual IEEE International Systems Conference (Sys- Con). IEEE, 2017, pp. 1-6.
20. Зегжда Д.П., Павленко Е. Ю. Гомеостатическая стратегия безопасности киберфизических систем / Д. П. Зегжда, Е. Ю. Павленко // Проблемы информационной безопасности. Компьютерные системы. 2017. № 3. С. 9–22.
21. Basan E., Basan A., Grutsynin A. Overview of Information Issues for a Robotic System. In Proceedings of 19th Interantional Conference on Communication Technology. IEEE, 2019, pp. 1275-1280.
22. Shyvakov O. Developing a security framework for robots // 2017. Pp.8-67.
23. Vilches V. M., Kirschgens L. A., et al. Introducing the robot security framework (RSF), a standardized methodology to perform security assessments in robotics //. Computer Science. 2018. Pp. 1-20.

AUTOMATION OF THE PROCESS OF ANALYSIS OF SECURITY THREATS IN CYBER-PHYSICAL SYSTEMS

Basan E.S.[5], Gritsynin A.S.[6], Shulika M.G.[7], Kryuchkov V.S.[8]

Purpose: *development of a methodology for automating the process of analyzing security threats in cyber-physical systems, which is based on the study and analysis of the system architecture and possible risks of threat implementation, as well as the capabilities of the intruder.*

Method: *the developed methodology is based on structuring information about the architectural features of cyber-physical systems. Structuring information and presenting it in the form of directories that are interconnected allows to determine the list of threats, vulnerabilities and attacks that are relevant to it based on structural and functional characteristics. When designing the database, an ontological approach was applied, which allows you to highlight concepts and their properties.*

Results: *methodological recommendations for analyzing the security of cyber-physical systems have been developed, based on the study and assessment of vulnerabilities and security threats. The analysis of the structural and functional characteristics of the cyber-physical system is carried out and the main features from the point of view of information security are highlighted. Integration of new methods for assessing risks, identifying current threats, and developing effective recommendations for cyber-physical systems made it possible to create a knowledge base about threats, attacks, vulnerabilities of CPS. New threats to CPS have been identified, which are associated with their specific properties: mobility, use of wireless networks, location outside the controlled area. The result of the study is a product presented in the form of a knowledge base that allows you to determine the degree of threat of a threat for a given structural and functional characteristics of a cyber-physical system. Implemented automatic updating of information about vulnerabilities from open databases.*

Keywords: *methodology, attacks, attack tools, structural and functional characteristics, threat base, ontology, concepts, risks, damage*

Reference

1. Makhdoom I., Lipman J., Ni. W. Anatomy of Threats to the Internet of Things // IEEE Communications surveys & Tutorials, vol. 21, no. 2, second quarter. 2019. Pp. 1636-1675.
2. Siboni S., Sachidananda V., Meidan Y., Bohadana M., Mathov Y., Bhairav S., Shabtai A., Elovici Y. Security Testbed for Internet-of-Things Devices. // IEEE transactions on reliability, 2019. №68 (1). Pp. 23-44.

5 Elena Basan, Ph.D., Associate Professor of the Department of Information Technology Security, Institute of Computer Technologies and Information Security, Southern Federal University “SFedU”, Taganrog, Russia. E-mail: ebasan@sfedu.ru, ORCID 0000-0001-6127-4484.

6 Anton Gritsynin, student of the Department of Information Technology Security, Institute of Computer Technologies and Information Security, Southern Federal University “SFedU”, Taganrog, Russia. E-mail: anton97_07@mail.ru

7 Maria Shulika, student of the Department of Information Technology Security, Institute of Computer Technologies and Information Security, Southern Federal University “SFedU”, Taganrog, Russia. E-mail: mshulika@sfedu.ru

8 Vasily Kryuchkov, assistant of the Department of Information Technology Security, Institute of Computer Technologies and Information Security, Southern Federal University “SFedU”, Taganrog, Russia. E-mail: kryuchkov@sfedu.ru

3. Atamli A.W., Martin A. Threat-based Security Analysis for the Internet of Things. In International Workshop on Secure Internet of Things. 2014, pp. 36-43.
4. Zhou W., Yu B. A Cloud-Assisted Malware Detection and Suppression Framework for Wireless Multimedia System in IoT Based on Dynamic Differential Game // China Communications. 2018. Pp. 209-223.
5. Carielli S., Eble M., Hirsch F., Rudina E., Zahavi R. IoT Security Maturity Model // Practitioner's Guide. Version 1.0. 2019. 129 p.
6. National Institute of Standards and Technology. Framework for Improving Critical Infrastructure Cybersecurity. Version 1.1. 2018. 55 p.
7. Sarfraz A., Mohammad M. R., Chowdhury J.N. Interoperability of Security Enabled Internet of Things // Wireless PersCommun. 2011. № 61. Pp. 567-586.
8. Tao M., Zuo J., Liu Z.; Castiglione A., Palmieri F. Multi-layer cloud architectural model and ontology-based security service framework for IoT-based smart homes. Future Gener // Computer Systems. 2018. № 78. Pp. 1040-1051.
9. Ekelhart A., Fenz S., Neubauer T. AURUM: A Framework for Information Security Risk Management. In Proceedings of the 2009 42nd Hawaii International Conference on System Sciences. IEEE, 2009; pp. 1-10.
10. Mozzaquatro B. A., Agostinho C., Goncalves D., Martins J., Jardim-Goncalves R.. An Ontology-Based Cybersecurity Framework for the Internet of Things //Sensors. 2018. № 18. Pp. 3053 -3055.
11. Abbass W., Bakraouy Z., Baina A., Bellafkih M. Classifying IoT security risks using Deep Learning algorithms. In 6th International Conference on Wireless Networks and Mobile Communications (WINCOM), 2018, pp. 1-10.
12. Fedorchenko A. V., Doynikova E. V., Kotenko I. V. Automated detection of assets and calculation of their criticality for the analysis of information system security // Tr. SPIIRAN. 2019. № 18(5). Pp. 1182-1211.
13. Electronic resource https://threatmodeler.com/ - access mode is free (Date of access 10.05.2021).
14. Bakhshi Z., Balador A., Mustafa J. Industrial IoT security threats and concerns by considering Cisco and Microsoft IoT reference models. In Wireless Communications and Networking Conference Workshops (WCNCW). IEEE, 2018, pp. 173-178.
15. Basan E., Basan A., Grutsynin A. Analysis of the Security Problems of Robotic Systems. In 2nd International Conference on Intelligent Communication and Computational Techniques (ICCT), 2019, pp. 1200-1214.
16. Electronic resource Facial Recognition Implemented at Beijing Capital International Airport – URL: https://medium.com/@pandaily/facial–recognition–implemented–atbeijing–capital– inter- national–airport–8c0b7cc1b945 (Date of access 12.03.2021).
17. Dieber B., Breiling B., Taurer S., Ka- cianka,S., Rass,S., Schartner P. Security for the Robot Operating System // Robot. Auton. Syst. 2017. № 98(C). Pp. 192–203.
18. National Institute of Standards and Technology, Framework for Improving Critical Infrastructure Cybersecurity, April 16, 2018, version 1.1, P.32-43.
19. Breiling, B., Dieber, B. and Schartner, P. Secure communication for the robot operating system. In Annual IEEE International Systems Conference (Sys- Con). IEEE, 2017, pp. 1-6.
20. Zegzhda D.P., Pavlenko E.Yu. Homeostatic strategy for the security of cyber-physical systems / D. P. Zegzhda, E. Yu. Pavlenko // Problems of information security. Computer systems. 2017. No. 3. S. 9-22.
21. Basan E., Basan A., Grutsynin A. Overview of Information Issues for a Robotic System. In Proceedings of 19th Interantional Conference on Communication Technology. IEEE, 2019, pp. 1275-1280.
22. Shyvakov O. Developing a security framework for robots // 2017. Pp.8-67.
23. Vilches V. M., Kirschgens L. A., et al. Introducing the robot security framework (RSF), a standardized methodology to perform security assessments in robotics.//. Computer Science. 2018. Pp. 1-20.