Вопросы защиты персональных данных в киберфизических системах

Людмила Сухостат
Институт Информационных Технологий НАНА, Баку, Азербайджан
lsuhostat@hotmail.com

***Аннотация*— Вопросы защиты персональных данных, характерные для киберфизических систем, являются одной из актуальных областей научных исследований. В статье представлен анализ существующих вопросов защиты персональных данных в киберфизических системах. Рассматриваются технологии и типы угроз, которым они подвержены. Приводятся некоторые решения этой сложной области исследований. Кроме того, рассматриваются открытые направления будущих исследований с целью защиты персональных данных, которые могут помочь исследователям в разработке новых подходов защиты от угроз киберфизическим системам.**

Ключевые слова— киберфизическая система; защита персональных данных; угрозы киберфизическим системам; взаимосвязь устройств; персональные данные

I. Введение

Киберфизические системы (Cyber-physical system, CPS) объединяют кибернетическое начало, аппаратные и программные средства компьютера, качественно новые исполнительные механизмы (актуаторы), встроенные в их среду и способные воспринимать изменения, реагировать на них, учиться и адаптироваться [1]. CPS способствует смене парадигмы от «взаимосвязанного» мира, в котором повседневные объекты становятся взаимозависимыми, к объектам способным напрямую общаться друг с другом и коллективно предоставлять интеллектуальные услуги [2].

Все эти объекты и их связь с окружающей средой несут с собой риск раскрытия личных данных и утечки информации. Беспроводная связь увеличивает риск нарушения из-за возможностей удаленного доступа, которые потенциально подвергают систему атакам прослушивания и маскировки.

Примеры секретных CPS данных включают физиологические данные, собранные биомедицинскими датчиками, данные о потреблении энергии, собранные интеллектуальными счетчиками, и данные о местоположении, собранные мобильными телефонами, и это лишь некоторые из них. Раскрытие таких данных может создать возможности для преступной активности или привести к серьезному ущербу или даже смерти. Поэтому с такой точки зрения CPS представляет собой серьезную проблему для безопасности, защиты персональных данных (ПД) и доверия, которые считаются одними из основных барьеров в разработке приложений CPS.

С непрерывным улучшением осведомленности о ПД, и промышленность, и научные круги активно разрабатывают жизнеспособные решения для удовлетворения постоянно растущих требований защиты ПД [3, 4].

Проблемы, связанные с защитой ПД, возникают во время процессов передачи, агрегирования и анализа данных, даже когда необработанные ПД недоступны, поскольку сложные методы интеллектуального анализа данных становятся все более эффективными и могут раскрыть основную информацию.

Традиционные технологии информационной безопасности в основном направлены на сохранение небольших и однородных ПД. Поэтому первостепенной задачей является разработка надежной, эффективной и масштабируемой аналитики больших данных с защитой ПД, которая может работать с крупномасштабными и разнородными данными [5]. Также необходимо найти компромисс между защитой ПД и полезностью, что означает, что люди все еще эффективно используют эти сервисы, в то же время, предотвращая раскрытие и вывод персональной информации, относящейся к конкретному человеку, в процессе анализа данных.

В последние несколько лет исследовательские сообщества ищут решения на данные вопросы и предложили множество подходов. Целью данной статьи является анализ уязвимостей существующих технологий CPS и угроз, направленных на нарушение защиты ПД.

В то время как область исследований все еще быстро развивается, также необходимо обсудить возможные решения вышеприведенных вопросов.

II. Защита Персональных Данных в CPS

Как философское понятие «защита ПД» может относиться к набору связанных, но разделяемых понятий [6], отслеживающих как описательные, так и нормативные компоненты [7, 8]. Защита ПД означает, что секретная информация об отдельных лицах или группах не раскрывается другим лицам.

DOI: 10.25045/NCInfoSec.2019.21

Хотя в некоторых контекстах защита ПД и конфиденциальность частично совпадают, они отличаются с точки зрения их концепций и методов защиты. Конфиденциальность рассматривается как «ориентированная на данные» концепция, которая означает, что речь идет о самих данных с целью обеспечения того, чтобы данные были известны только уполномоченным сторонам [8]. Тогда как защита ПД включает в себя дополнительную концепцию, «ориентированную на владельцев данных», которые могут быть отдельными лицами или группами, с целью защиты их частной информации при использовании их данных для анализа [8]. Следовательно, концепция защиты ПД включает рассмотрение компромисса между открытыми данными и анонимностью. Различия в их концепциях приводят к различиям в методах их защиты. Шифрование является одним из таких методов защиты [9]. Помимо криптографических инструментов, защита ПД также поддерживается методами возмущения (perturbation) (для скрытия истинного значения данных) и анонимизации (для скрытия связи «данные – владелец данных»). Другое отличие состоит в том, что потеря конфиденциальности в основном вызвана слабостью контроля доступа или схем шифрования, в то время как потеря защиты ПД связана также с уязвимостями в управлении использованием данных и аналитикой данных.

Пользователи CPS сталкиваются с угрозами защиты ПД при передаче личной информации через Интернет. Из-за большого числа устройств в CPS необходимо учитывать различные риски перед разработкой приложений или решений.

III. Влияние Технологий CPS на Защиту Персональных Данных

Сенсоры, устройства, данные, компьютеры и облачные соединения в значительной степени зависят от установленных доверительных отношений. Подключение большого количества устройств CPS (т. е. добавление точек вторжения) повышает вероятность угрозы для данной системы, тем самым увеличивая общий риск безопасности. Без возможности ограничения настроек для защиты ПД трудно установить доверие с системой или устройством CPS.

С точки зрения обеспечения защиты ПД на Рис. 1 представлены наиболее важные технологии CPS [10]:

Число устройств. Увеличение числа связанных устройств в CPS приводит к серьезным проблемам, в частности, масштабируемости существующих и будущих технологий защиты ПД.

Взаимосвязь устройств. С технологическим прогрессом и снижением затрат на беспроводную связь устройства CPS становятся доступными для запросов с любого расстояния, что дает большие возможности для новых услуг, но вызывает проблемы с защитой ПД.

Сбор данных. С ростом числа интеллектуальных устройств сбор данных еще глубже проникает в жизнь людей и вводит новые наборы связанных и идентифицируемых личных данных. При этом люди пассивны и, в основном, не знают о сборе данных в результате роста числа подключенных устройств.

Взаимодействие устройств. Интерфейсы позволяют людям осуществлять настройку, отладку и взаимодействие с интеллектуальными устройствами. Так развитие технологий привело к переходу от RFID (Radio Frequency IDentification) меток к сенсорам, реагирующим на прикосновения. Отсутствие интерфейсов и механизмов взаимодействия может создавать угрозы для личных данных. А сложные интерфейсы, например, на основе речевых технологий или даже телепатии приведут к расширению проблем защиты ПД.

Взаимодействие систем с людьми. Взаимосвязь и координация множества устройств и их специфических возможностей служит взаимодействию с людьми на основе сложных интерфейсов. Разработка последних требует тщательной подготовки, чтобы не нарушить защиту ПД.

Жизненный цикл устройств. CPS хранят обширную информацию о своей собственной истории в течение всего их жизненного цикла [10]. Они становятся все более динамичными при обмене информацией, например, в медицинских устройствах. С увеличением срока хранения данных и переходов в течение жизненного цикла, управление аспектами безопасности и защиты ПД станет более сложным.

Переход от вертикальной интеграции решений к горизонтальной. Современные CPS системы сочетают в себе вертикальные и горизонтальные интегрированные решения, например, интеллектуальные счетчики, которые не только передают данные о потреблении центральному коммунальному поставщику (вертикальная интеграция), а напрямую включают и выключают бытовые приборы (горизонтальная интеграция).

Локальность информационных потоков в горизонтально интегрированных системах в большей степени защищает ПД. А вертикальное интегрирование систем с различными целями и производителями может вызвать угрозы защиты ПД и нарушения безопасности.

IV. Угрозы Защиты Персональных Данных в CPS

Вопросы безопасности и защиты ПД, характерные для CPS и данных временных рядов, передаваемых из них, представляют собой новые области научных интересов.

Существуют как преимущества, так и недостатки безопасности, основанные на сложности главной вычислительной проблемы и информационной теоретической безопасности.

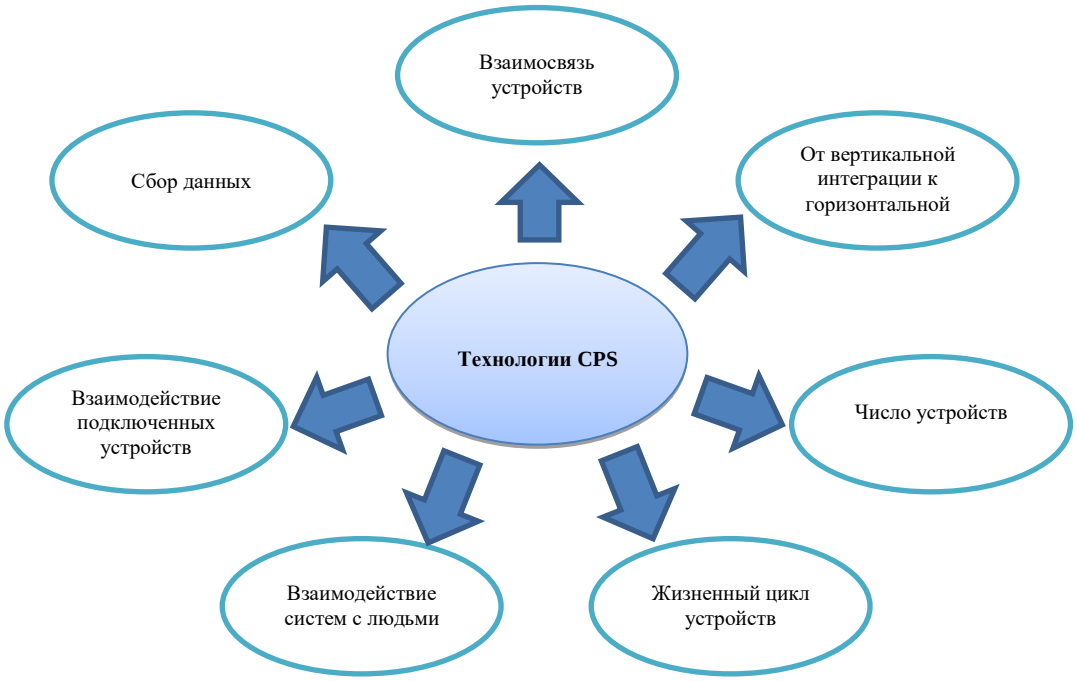

Рис. 1. Технологии CPS, подвергающие опасности защиту персональных данных.

Основной мерой теоретико-информационной безопасности является внутренняя информация, доступная для использования злоумышленником, независимо от того, каким образом злоумышленник ее использует.

Несмотря на множество потенциальных преимуществ, CPS представляет значительную угрозу защите ПД и безопасности из-за используемых технологий [10, 11]. Существует различные угрозы защиты данных пользователей и сложности, связанные с противостоянием таким угрозам (Таблица I), а именно:

- *Идентификация*

Персональная информация может передаваться, когда объект связан с человеком прямо или косвенно. Связь возникает, если пользователь осведомлен и дает согласие на возможную передачу личных данных. Например, когда человек что-то покупает с использованием пластиковой карты. Это может стать риском для защиты ПД пользователя.

- *Профилирование*

Угроза профилирования растет при движении к интеллектуальным сетям (smart grid) и городам. Примером является внедрение интеллектуальных электрических счетчиков, которые передают данные о потреблении энергии соответствующим коммунальным предприятиям с целью мониторинга и выставления счетов.

С юридической точки зрения необходимо учитывать вопросы, такие как профилирование потребителей, потеря данных, утечка данных и отсутствие согласия (согласие является обязательным по закону).

- *Локализация и отслеживание*

Смартфоны и другие мобильные устройства, подключенные к Интернету, ежедневно распространяют данные, которые могут быть незаконно использованы другими людьми. Так легко можно найти точные данные о местоположении пользователя с применением геолокации. Таким образом, защита ПД может быть нарушена.

- *Переходы жизненного цикла*

Эта угроза связана со сбором и хранением информации, которая может многое рассказать об образе жизни людей, в т.ч. о местоположении, медицинских данных и др. Устройства CPS имеют динамичный жизненный цикл, где ими можно обмениваться, добавлять и свободно распоряжаться. Необходимо разработать гибкие решения для реализации «удобных» механизмов управления жизненным циклом защиты ПД.

- *Атаки на ресурсы*

Данный вид угрозы направлен на несанкционированный сбор информации о существовании и характеристиках личных данных. Информация об устройствах может быть получена законными лицами (например, владельцем и авторизованными пользователем) из различных источников, нелегитимные стороны могут запрашивать и использовать это для составления списка устройств и их местонахождения (дом, офис, предприятие). Даже если CPS могут отличить законные

запросы от незаконных (данные по скорости их общения, времени реакции и других уникальных характеристик), они могут потенциально использоваться для определения их типа и модели. Применение технологий беспроводной связи позволяет проводить атаки пассивно с применением подслушивающих устройств в непосредственной близости от дома жертвы. Например, грабители могут использовать информацию о ресурсах с целью незаконного проникновения в частные владения, промышленный шпионаж и т.д.

- *Связь систем*

Эта угроза состоит в объединении различных ранее разделенных систем. Пользователи боятся неправильного суждения и потери контекста, когда данные, собранные от разных сторон в разных контекстах и разрешениях, объединяются.

Обход механизмов защиты ПД приводит к росту риска несанкционированного доступа и утечки частной информации. Примером может служить возрастающий риск повторной идентификации анонимизированных данных.

V. Решения по Защите Персональных Данных в CPS

Растущие угрозы защиты ПД приводят к необходимости разработки подходов и контрмер, направленных на борьбу с ними.

В связи с этим существует ряд подходов по защите ПД в CPS, которые можно классифицировать следующим образом [12, 13]:

- Шифрование данных;
- Контроль доступа;
- Закон и политика;
- К-анонимность;
- Кэширование;
- Фиктивные запросы;
- Запутывание программного кода

и т.д.

Существуют и гибридные методы, такие как шифрование с запутыванием, кэширование с фиктивными запросами и др. [13].

Так решением для угрозы переходов жизненного цикла является временная блокировка персональной информации. А атакам на ресурсы можно противостоять, применяя легковесную криптографию и устойчивые механизмы снятия «отпечатков» устройств.

ТАБЛИЦА I. Влияние Технологий CPS на Угрозы Защиты Персональной Информации

Угрозы Защиты Персональных Данных в CPS	**Вид Угрозы**	**Виды Нарушений**	**Сложности**
	Идентификация	Распознавание по лицу, отпечаткам пальцев, речи и др.	Преобладание локальной обработки данных над централизованной; Преобладание горизонтальной коммуникации над вертикальной; Осведомленность пользователей.
	Локализация и отслеживание	GPS отслеживание; Интернет трафик; Определение местоположения по телефону.	Осведомленность о слежении перед пассивным сбором данных; Управление обменом локальными данными в помещении; Протоколы интеллектуального анализа с целью защиты ПД для взаимодействия с CPS системами.
	Профилирование	Рекомендательные системы; Информационные бюллетени; Рекламные объявления.	Рост объемов данных; Сбор данных из частной жизни людей.
	Угроза взаимодействия и представления	Неприкосновенность информации о частной жизни; Среда представления.	Раскрытие информации при взаимодействии устройств
	Переходы жизненного цикла	Сбор информации; Динамичный обмен информацией.	Обмен данными между устройствами
	Атаки на ресурсы	Сбор информации; Незаконные действия правоохранительных органов; Промышленный шпионаж.	Проверка подлинности запросов; Устойчивость к цифровому «отпечатку».
	Связь систем	Потеря контекста; Гетерогенная распределенная система систем; Риск повторной идентификации анонимизированных данных.	Прозрачность в отношении того, какой информацией система систем обменивается с кем-либо; Модели разрешений и контроля доступа должны быть адаптированы для множества заинтересованных сторон; Методы анонимизации данных должны работать на связанных системах и быть устойчивыми.

Решениями для профилирования будут:

- Персонализация на стороне клиента;
- Запутывание программного кода;
- Анонимизация;
- Шифрование данных.

Исследование по локализации и отслеживанию сосредоточено на следующих методах защиты:

- Изменение возможных зон расположения пользователя.
- Добавление случайного шума к информации о местоположении.

Таким образом, в статье был проведен анализ возможных решений с целью защиты ПД от угроз на CPS, которые необходимо преодолеть.

Заключение

Несмотря на то, что в последние годы исследователи приложили немало усилий к вопросам защиты ПД в CPS, эта область все еще остается неопровержимо сложной и оставляет место для совершенствования существующих подходов, а также для разработки новых решений. В работе были рассмотрены виды угроз направленные на снижение защиты ПД, классификация технологий CPS и некоторые пути решения по защите от угроз.

Несмотря на значительный прогресс, достигнутый в области защиты ПД, остается еще много нерешенных проблем. Ряд вопросов будущих исследований приводится ниже:

- Разработка приложений по обеспечению защиты ПД в рамках различных сценариев угроз.
- Рассмотрение вопроса о ПД для приложений в распределенной среде с многочисленными устройствами с ограниченными ресурсами, такими как мобильные социальные сети, интеллектуальные счетчики, медицинские устройства и т.д.
- Разработка метода на основе легковесной криптографии с целью повышения практической эффективности.

Исследование методов устойчивых к всевозможным типам атак на ПД с различными предположениями о знаниях злоумышленника.

Литература

[1] R. Alguliyev, Y. Imamverdiyev, L. Sukhostat, “Cyber-physical systems and their security issues,” Computers in Industry, vol. 100, 2018, pp. 212–223.

[2] A.A.A. Sen, F.A. Eassa, K. Jambi, M. Yamin, “Preserving privacy in internet of things: A survey,” International Journal of Information Technology, vol. 10, 2018, pp. 189–200.

[3] P. Zikopoulos, C. Eaton, “Understanding Big Data Analytics for Enterprise Class Hadoop and Streaming Data,” McGraw-Hill Osborne Media, First Edition, 2012, 176 p.

[4] S. LaValle, E. Lesser, R. Shockley, M.S. Hopkins, N. Kruschwitz, “Big data, analytics and the path from insights to value,” MIT Sloan Management Review, Vol. 52, no. 2, 2011, pp. 21-31.

[5] J.A. Shamsi, M.A. Khojaye, “Understanding privacy violations in big data systems,” IT Professional, Vol. 20, no. 3, 2018, pp. 73–81.

[6] A. Moore, “Defining privacy,” Journal of Social Philosophy, Vol. 39, no. 3, 2008, pp. 411-428.

[7] A. Henschke, “Ethics in an Age of Surveillance: Personal Information and Virtual Identities,” Cambridge University Press, Cambridge, 2017, 334 p.

[8] F. Allhoff, A. Henschke, “The internet of things: Foundational ethical issues,” Internet of Things Vol. 1-2, 2018, pp. 55-66.

[9] N. Li, N. Zhang, S.K. Das, B. Thuraisingham, “Privacy preservation in wireless sensor networks: a state-of-the-art survey,” Ad Hoc Networks, Vol. 7, no. 8, 2009, pp. 1501–1514.

[10] J. Ziegeldorf, O. Garcia-Morchon, K. Wehrle, “Privacy in the Internet of Things: threats and challenges,” Security and Communication Networks, Vol. 7, no. 12, pp. 2728–2742.

[11] N. Fabiano, “Internet of Things and the Legal Issues related to the Data Protection Law according to the new European General Data Protection Regulation,” Athens Journal of Law, Vol. 3, no. 3, 2017, pp. 201-214

[12] V. Chellappan, K.M. Sivalingam, “Security and privacy in the Internet of Things,” in: *Internet of Things*, A.V. Dastjerdi, R. Buyya, Ed. Morgan Kaufmann, 2016, pp. 183-200.

[13] M. Yamin, Y. Alsaawy, A.B. Alkhodre, A.A.A. Sen, “An Innovative Method for Preserving Privacy in Internet of Things,” Sensors, Vol. 19, 2019, pp. 1-24.

PRIVACY ISSUES IN CYBER-PHYSICAL SYSTEMS

Lyudmila Sukhostat

Institute of Information Technology of ANAS, Baku, Azerbaijan

lsuhostat@hotmail.com

Abstract— Personal data protection issues specific to cyber-physical systems are one of the relevant areas of scientific research. The paper presents an analysis of existing issues of personal data protection in cyber-physical systems. The technologies and types of threats to which they are exposed are considered. Some solutions to this complex research field are presented. Also, open directions for future research with the aim of privacy that can help researchers to develop new approaches in protecting against threats to cyber-physical systems are considered.

Keywords— *cyber-physical system; privacy; cyber-physical system threats; device interconnection; personal data*