О защите персональных данных в системах, реализуемых на основе концепции Industry 4.0

Тахмасиб Фаталиев[1], Шакир Мехтиев[2]
[1,2]Институт информационных технологий НАНА, Баку, Азербайджан
[1]*depart3@iit.science.az*, [2]*shakir@iit.science.az*

***Аннотация*– Промышленные революции играют важную роль в развитии критических систем. Четвертая промышленная революция, или Industry 4.0 произвела кардинальные изменения в этой области, и в большей степени обязана появлению и развитию Интернета вещей, киберфизических систем, искусственного интеллекта, робототехники и других передовых технологий. Они привели к созданию полностью автоматизированного цифрового производства, управляемого интеллектуальными системами в режиме реального времени в постоянном взаимодействии с внешней средой. По сути, эти технологии делают производственную систему “умной сетевой фабрикой”, где вся деятельность контролируется цифровым способом, и, в результате, использование финансовых и материальных ресурсов становится более эффективным. Наряду с этим, увеличение сбора и обработки больших объемов данных, а также высокая степень автономности и децентрализации для таких систем являются факторами, которые могут стать проблематичными в контексте защиты данных и, в первую очередь, персональных данных. Данная работа посвящена вопросам защиты персональных данных в системах нефтегазового комплекса, реализуемых на основе концепции Industry 4.0. Рассмотрены концептуальные задачи и даны рекомендации по их решению.**

Ключевые слова– промышленная революция; Industry 4.0; персональные данные; нефтегазовый комплекс; риск; защита данных

I. Введение

Отличительной чертой информационного общества является взрывной рост данных. Интернет, наука, медицина, финансы, розничная торговля, видеонаблюдение и другие отрасли создали огромное количество данных. На производстве различные контрольно-измерительные приборы производят бесконечный поток данных. Наряду с этим, интеллектуализация производства при широкой степени интеграции сетевых и коммуникационных технологий увеличила потенциал стороннего доступа и, следовательно, в этом контексте возник также целый ряд проблем в отношении вопросов безопасности информации и связи. Благодаря интеграции новых методов сбора и анализа данных, а также путем тщательного мониторинга опыта клиентов и их предпочтений производители стали собирать их персональные данные (ПД) об использовании своих продуктов в целях удовлетворения растущих потребностей конечных потребителей. Т.е. среди всех данных особая роль стала отводиться ПД. Многие технологические компании (Facebook, Google) и организации собирают, обрабатывают, используют и распространяют ПД без ограничений. Кроме того, некоторые предприятия обмениваются данными пользователей с третьей стороной. И в большинстве случаев пользователь даже не осознает моменты, когда его ПД используются без согласия. По оценкам специалистов данные являются ценным корпоративным ресурсом компаний, и руководители должны делать все, чтобы защитить собственные данные и обеспечить конфиденциальность данных сотрудников и клиентов [1]. Вышеуказанные проблемы не обошли стороной и нефтегазовый комплекс (НГК). В данной работе освещаются некоторые вопросы защиты ПД в технических системах НГК, реализованных на основе концепции Industry 4.0.

II. Industry 4.0 и Проблемы Кибербезопасности

Существующий научно-технический уровень современной цивилизации в большой степени связан с произошедшими на протяжении последних двухсот пятидесяти лет промышленными революциями (ПР). До сих пор различали четыре ПР. В настоящее время мы находимся в стадии четвертой ПР, известной теперь как Industry 4.0, и перманентно переходящей в Industry 5.0. Industry 4.0 стала возможной благодаря таким прогрессивным технологиям, как системы радиочастотной идентификации (Radio Frequency IDentification, RFID), беспроводные сенсорные сети (Wireless Sensor Networks, WSN), системы межмашинного взаимодействия (Machine-to-Machine, M2M), Интернет вещей (Internet of Things, (IoT), большие данные (Big data), а также облачные сервисы (cloud computing), озеро данных (data lake) и искусственный интеллект Artificial Intelligence, AI) [2]. В Industry 4.0 цифровизация и объединение технических систем сделали возможным слияние физического и виртуального мира в области производства и логистики в так называемые киберфизические системы (КФС). Технические системы приобрели способность автономно обмениваться друг с другом данными и, таким образом, оптимизировать протекание процессов. При этом, в Industry 4.0 особая роль отводится созданию сенсорных сетей в промышленном секторе. Так называемые сенсоры 4.0 являются не только источниками первичных измерительных данных, но и предоставляют

DOI: 10.25045/NCInfoSec.2019.11

децентрализованные вычислительные мощности и программируемость [3, 4].

Отметим, что в Industry 4.0 физические объекты и процессы контролируются и управляются посредством КФС. Важно представить, что здесь могут использоваться объединенные или индивидуальные системы управления. Данные с сенсоров, такие как температура, давление, плотность вещества и др. используются в системе для контроля и управления. Увеличение сбора и обработки больших объемов данных, а также высокая степень автономности и децентрализации управляющих систем в Industry 4.0 стали факторами, которые оказали влияние и на кибербезопасность. Традиционно кибербезопасность направлена на защиту людей и организаций от таких угроз, как вредоносные программы, атаки социальных инженеров, порча веб-сайтов и т.д. [5]. В последнее время наблюдается рост сложности и интенсивность кибератак, которые ориентированы на финансовые преступления, промышленный шпионаж и время от времени даже направлены против правительств и критически важной инфраструктуры. В эпоху Industry 4.0 организации сильно связаны со своими интеллектуальными устройствами и сетями. Это представляет собой очень выгодную цель для киберпреступников, которые находят гораздо более простые точки входа в сети и устройства. Кибератаки на критически важную инфраструктуру и стратегические промышленные сектора стали более частыми и изощренными. Они не только приводят к нарушению нормального функционирования общества, но и наносят вред моральному духу пострадавших стран [6]. Например, Украина столкнулась с множеством таких атак на энергосистему, что привело к отключению электроэнергии в некоторых регионах.

Непрерывное совершенствование электронных технологий привело к тому, что в современном обществе, как на уровне правительств, так и в гражданском обществе, стали осознавать риски, создаваемые от использования личной информации. Прогресс науки и техники расширил жизненное пространство людей и дал им большую свободу поведения. Облачные вычисления позволяют хранить личную информацию вдали от нашего телефона, ноутбука или любых других персональных терминалов, что позволяет пользователю получать доступ к информации из любого места на любом устройстве. Наоборот, способность пользователя контролировать эту информацию значительно снизилась. Более того, мобильный интернет собирает информацию повсеместно, особенно персонализированную информацию, такую как контакты, фотографии и электронные письма. Однако, если популяризация облачных вычислений и мобильного интернета только усиливает сложность защиты информации на количественном уровне, то появление больших данных в настоящее время разрушает основу системы защиты личной информации с качественного уровня, что нельзя недооценивать. Например, в настоящее время технологии профилирования используются повсеместно для поиска скрытых закономерностей и взаимосвязей публики. Кроме того, они позволяют повторно идентифицировать личные данные, что делает стратегию анонимизации менее эффективной и ставит под сомнение фундаментальный принцип защиты данных.

Функционирование структур нефтегазового комплекса, реализованного на основе концепции Industry 4.0, можно представить, как умное производство (smart manufacturing) [7], в котором риски в основном возникают также и в сфере обработки ПД, касающихся персонала и клиентов. Каждый случай сетевого взаимодействия между людьми и производственными и логистическими системами может привести к тому, что личные данные будут получены, обработаны и при определенных обстоятельствах переданы вместе с другими данными. Риски потери данных на умном производстве могут быть связаны и с системами помощи персоналу, такими как планшеты, смартфоны, очки виртуальной и дополненной реальности и портативные терминалы данных. Они могут помочь персоналу избежать ошибок, предоставив им соответствующую справочную информацию, т.е. используются исключительно в производственных процессах. Однако, в этом случае ПД, например, координаты местоположения могут быть отслежены, и тогда необходимо принять защитные меры, начиная с технического уровня.

В Общем регламенте по защите данных, известном как General Data Protection Regulation (GDPR), предложен ряд мер по защите ПД в контексте внедрения Industry 4.0 [8]. Также в трудовых законодательствах ряда стран предусматриваются различные меры наказаний и штрафов по ненадлежащему использованию ПД. Так, в Трудовом кодексе Азербайджана предусмотрены организационные, физические и технические (аппаратные) меры для защиты личной информации от несанкционированного и случайного доступа, уничтожения, изменения и копирования.

III. Характеристики Персональных Данных и Риски Безопасности в Нефтегазовом Секторе

Рассмотрим общие характеристики ПД, которые являются универсальными и применимы, в том числе, и в НГК. Согласно GDPR к ПД можно отнести любую информацию, относящуюся к идентифицированному или идентифицируемому физическому лицу. Статистические данные, включая данные, относящиеся к физическим лицам, не считаются ПД при условии, что они действительно анонимны, то есть физические лица не могут быть идентифицированы.

Любые операции, выполняемые с ПД или с наборами ПД, независимо от того, выполняются ли они автоматическими средствами, такими как сбор, запись, организация, структурирование, хранение, адаптация или изменение, поиск, консультация, использование, раскрытие путем передачи, распространение или иное предоставление, выравнивание или комбинация, ограничение, удаление или уничтожение– квалифицируется как обработка ПД. Таким образом, очевидно, что проблемы с ПД могут возникать во всех сферах деятельности и во всех аспектах жизни в целом, поскольку информацию, с помощью которой можно

идентифицировать физических лиц, можно найти практически везде.

На основании проведенного анализа можно выделить следующие категории ПД:

А. Личные данные– к ним относятся:

- контактная информация– инициалы, название компании, должность, рабочие и мобильные телефоны, рабочий и личный адрес электронной почты и почтовый адрес.
- Профессиональные данные– сведения об истории работы и карьеры, образовании и профессиональном членстве, опубликованные статьи, а также сведения по страхованию и пенсионному обеспечению.
- Финансовая информация– к этой подгруппе личных данных можно отнести налоги, платежные ведомости, инвестиционные интересы, пенсии, активы, банковские реквизиты, записи о банкротстве.

Б. Чувствительные ПД:

- Документы, удостоверяющие личность, которые могут выявить расу, религию или этническое происхождение, политические взгляды.
- Любая информация, раскрывающая данные о здоровье или данные, касающиеся личной жизни физического лица, информация о нахождении под следствием, осуждении за совершение преступления.
- Биометрические данные.

В. Данные, защищенные правом интеллектуальной собственности (авторское право, закон о товарных знаках, закон о базе данных, патентный закон) и *полученные на основе обработки географических местоположений.*

Методы защиты ПД должны быть направлены на устранение утечек или на уменьшение негативных последствий. К наиболее известным и распространенным видам утечек данных можно отнести следующие их виды:

Умышленные утечки: основной их причиной становятся действия сотрудников, имеющих доступ к секретам легально, в силу своих служебных обязанностей.

Кража информации (извне): взлом компьютера с помощью вредоносных программ и хищение информации с целью использования в корыстных интересах (хакерские атаки).

Кражи носителей данных: преднамеренные кражи ноутбуков, смартфонов, планшетов и съемных носителей данных в виде флешь-памяти, жестких дисков.

Случайные утечки: происходят из-за потери носителей данных (флешь-памяти, ноутбуков, смартфонов и т.п.) или ошибочных действий сотрудников организации. Такой вид утраты случается в результате ошибочного размещения конфиденциальной информации в Интернет.

Социальная инженерия: основана на социальных и психологических приемах, позволяющих так называемым социальным хакерам получить доступ к закрытым данным внутри организации от ничего не подозревающих сотрудников, попавших на их уловки.

Следует отметить, что, независимо от вида деятельности, любая организация, которая в своей деятельности обрабатывает ПД, обязана предпринять комплекс административных и технических мер, направленных на их защиту. Политика безопасности предприятия должна обеспечивать необходимые механизмы управления рисками безопасности.

IV. Некоторые Концептуальные Вопросы Защиты Персональных Данных в Industry 4.0

Рассмотрим основные проблемы, возникающие в технических системах промышленности, в том числе и нефтегазового сектора, реализованных на основе концепции Industry 4.0. К ним можно отнести следующие группы проблем:

1. *Производственно-технологические проблемы*– управление и оптимизация производственных процессов, внедрение сенсоров на новых физических принципах, техническое обслуживание и др.
2. *Информационно-технологические проблемы*– автоматизация технологических процессов, системы типа SCADA, Интернет вещей, беспроводные сенсорные сети, искусственный интеллект, виртуальная и дополненная реальности.
3. *Разработка и внедрение программных средств*.
4. *Сбор, обработка и передача данных, Big data аналитика.*
5. *Вопросы безопасности*– непрерывная и устойчивая деятельность производственных циклов, экологическая безопасность, охрана жизни и здоровья персонала, информационная безопасность предприятий и защита ПД.

Каждая из рассмотренных проблем является сложной и ответственной задачей, требующей отдельных исследований. Рассмотрим часть проблем, которые могут возникнуть из-за уязвимостей в информационной безопасности ПД на предприятиях НГК, реализованных на основе концепции Industry 4.0.

Здесь деструктивная деятельность может иметь значительные негативные последствия, в особенности, в странах, имеющих существенную нефтегазовую составляющую. Эти действия направлены как на сотрудников компаний, так и на информационную безопасность компаний. В первом случае это могут быть действия преступных группировок с целью кражи денег с банковских счетов, шантаж с вымогательством денег, дискредитация. Во втором случае через ПД атакам подвергается информационная безопасность компаний. Применительно к нефтегазовому сектору атакам подвергаются как материальные, так и нематериальные активы компаний. Например, используя чувствительные ПД ключевых сотрудников, посредством их шантажа можно вызвать проблемы с оборудованием вплоть до остановки процесса добычи. Рискам подвергаются также

производственные и технологические процессы. В случаях осуществления подобных сценариев кибератак возможные аварии и загрязнения окружающей среды могут нанести миллионные убытки и урон репутации компании и их продукции и вызвать возрастающий общественный резонанс. На основе обработки данных о географическом положении сотрудников компании можно получить сведения о перспективных месторождениях нефти и газа. Также в результате утечек и кражи ПД можно получить конфиденциальные сведения коммерческого характера, о тендерной деятельности, данные договоров с партнерами и подрядчиками, условия работы и др. Возможный ущерб от таких утечек может выражаться в упущенной выгоде в результате испорченного имиджа; в компенсации по судебным искам; в снижении котировок акций; в стоимости проигранных тендеров и в других финансовых потерях. Таким образом, резюмируя вышеизложенное, отметим, что известные методы защиты данных, также применимы и к ПД. Среди них обычно выделяют четыре основные группы методов: правовые, организационные, технические, программно-аппаратные.

На любом объекте Industry 4.0 должна действовать политика безопасности. Одной из составных частей политики безопасности должно быть обеспечение защиты ПД. Политика безопасности должна быть разработана с учетом требований международных норм, стандартов и должна соответствовать внутригосударственным правовым актам, нормативным документам и законам. Особенно следует отметить, что в существующем законодательстве могут быть отражены не все аспекты в области защиты ПД. Учитывая динамичный характер развития современных ИКТ и их возросшее влияние во всех сферах деятельности, может потребоваться коррекция как существующих законов, так и методов защиты ПД.

Заключение

Защита ПД в структурах НГК, реализуемого на основе концепции Industry 4.0, играет важную роль в производственной сфере и обеспечении конкурентоспособности. Проведенный анализ в этой области показал, что исследуемая задача является критичной и актуальной. Каждый случай сетевого взаимодействия между людьми и производственными и логистическими системами может привести к тому, что ПД будут получены, обработаны и при определенных обстоятельствах переданы вместе с другими данными. При этом резко возрастают риски утечек ПД и случайное или преднамеренное их использование в корыстных целях. Инструменты информационных-коммуникационных технологий могут помочь персоналу избежать ошибок, предоставив им соответствующую информацию. Однако, предоставляемые ПД могут использоваться исключительно для оптимизированного планирования и управления, но не для мер, касающихся трудового законодательства. Это также необходимо учитывать при использовании новых технологий в производственных процессах. Если данные персонала или клиента могут быть отслежены, необходимо принять эффективные защитные меры.

Благодарности

Данная работа выполнена при финансовой поддержке Фонда науки Государственной нефтяной компании Азербайджана SOCAR- **Контракт № 03 LR-AMEA.**

Литература

[1] “Compliance in the Era of Globetrotting Data”. https://www.intel.com/content/www/us/en/business/enterprise-computers/gdpr-compliance.html

[2] Y. Lu, “Industry 4.0: A survey on technologies, applications and open research issues”, Journal of Industrial Information Integration, No. 6, pp. 1–10, 2017.

[3] A. Schütze, N. Helwig, and T. Schneider, “Sensors 4.0– smart sensors and measurement technology enable Industry 4.0”, Journal of Sensors and Sensors Systems, No. 7, pp. 359-371, 2018.

[4] T. Kh. Fataliyev, Sh. A. Mehdiyev, “Analysis and new approaches to the solution of problems of operation of oil and gas complex as cyberphysical system”, International Journal of Information Technology and Computer Science (IJITCS), Vol. 10, No. 11, pp. 67-76, 2018.

[5] J. Jang-Jaccard, S. Nepal, “A survey of emerging threats in cybersecurity”, Journal of Computer and System Sciences, Vol. 80, Issue 5, pp. 973-993, 2014.

[6] Т. Фаталиев, Ш. Мехтиев, “Вопросы обеспечения энергетической безопасности инфраструктуры электронной науки”, 4-я Республиканская конференция по информационной безопасности, сс. 105-108, 2018.

[7] T. Kh. Fataliyev, Sh. A. Mehdiyev, “Integration of cyber-physical systems in e-science environment: state-of-the-art, problems and effective solutions”, International Journal of Modern Education and Computer Science(IJMECS), Vol.11, No. 9, pp. 35-43, 2019.

[8] General Data Protection Regulation (GDPR). Official Journal of the European Union, 2016, pp. 1-88.

ABOUT PROTECTION OF PERSONAL DATA IN INDUSTRY 4.0 BASED SYSTEMS

Tahmasib Fataliyev[1], Shakir Mehdiyev[2]
[1,2]Institute of Information Technology of ANAS, Baku, Azerbaijan
[1]depart3@iit.science.az, [2]shakir@iit.science.az

Abstract— Industrial revolutions play an important role in the development of critical systems. The fourth industrial revolution, or Industry 4.0, has made the cardinal changes in this area, and is more indebted by the emergence and development of the Internet of things, cyber-physical systems, artificial intelligence, robotics and other advanced technologies. They led to the creation of a fully automated digital production controlled by real-time intelligent systems in constant interaction with the external environment. In essence, these technologies make the production system a “smart network factory”, where all activities are digitally controlled, and, as a result, the use of financial and material resources are becoming more efficient. Along with these, an increase in the collection and processing of large volumes of data, as well as a high degree of autonomy and decentralization for such systems, are factors that can become problematic in the context of data protection and, first of all, personal data. This work is devoted to the protection of personal data in oil and gas sector systems, implemented on the basis of the Industry 4.0 concept. Conceptual tasks are considered and recommendations for their solution are given.

Keywords— *industrial revolution; Industry 4.0; personal data; oil and gas sector; risk; data protection*