УДК: 332
DOI: 10.52531/1682-1696-2022-22-2-116-122
Научная статья

ИНТЕРНЕТ ВЕЩЕЙ И КОМПЛАЕНС-КОНТРОЛЬ

Н.Ш. Иванченко[1], Д.С. Лепешкин[1], М.А. Кульгускина[1], А.Ф. Гиниятуллин[2]
[1] Высшая школа промышленной политики и предпринимательства, РУДН
[2] Институт региональных экономических исследований

В статье рассмотрены основные направления организации и проведения комплаенс-контроля при использовании и применении в организации технологии Интернет вещей (англ. internet of things, IoT) на предмет информационной безопасности.

В процессе исследования авторы выделяют основные направления и проблемные зоны IoT (сети передач данных между физическими объектами – («вещами»), которые нуждаются в постоянном мониторинге и модернизации. В результате проведенного анализа авторы подготовили и сформулировали четыре основных шага при проведении комплаенс-контроля рассматриваемой области: определить требования, осуществить анализ рисков, провести тестирование и осуществлять систематические проверки системы. В целях минимизации риска взаимодействия пользователей авторами подготовлены рекомендации, которые необходимо осуществлять на постоянной основе при использовании технологий IoT, а именно строгому контролю подлежат следующие характеристики и возможности системы IoT: срок годности (продукта или услуги), способы и надежность авторизации и аутентификации, хранение и защита данных, осуществимость комплексного тестирования, наличие гибкости системы, допустимость удаленного администрирования, обнаружение аномалий, соответствие применяемых стандартов отрасли, для которой разрабатывался продукт или услуга IoT.

Ключевые слова: *интернет вещей (internet of things, IoT), комплаенс-контроль, it-система, информационная безопасность, протокол.*

Original article

INTERNET OF THINGS AND COMPLIANCE CONTROL

N.Sh. Ivanchenko[1], D.S. Lepeshkina[1], M.A.Kulguskina[1], A.F. Giniyatullin[2]
[1] Higher School of Industrial politics and entrepreneurship, RUDN University,
[2] Institute of Regional economic research

The article examines the main directions of the organization and conduct of compliance control in the use and application of Internet of Things technology (English Internet of things, IoT) in the organization for information security.

In the course of the study, the authors identify the main areas and problem areas of IoT (data transmission networks between physical objects («things»)) that need constant monitoring and modernization. As a result of the analysis, the authors prepared and formulated four main steps in conducting compliance control of the area under consideration: to determine requirements, to carry out risk analysis, to conduct testing and to carry out systematic checks of the system. In order to minimize the risk of user interaction, the authors have prepared recommendations that must be implemented on an ongoing basis when using IoT technologies, namely, the following characteristics and capabilities of the IoT system are subject to strict control: shelf life (of a product or service), methods and reliability of authorization and authentication, data storage and protection, feasibility of comprehensive testing, availability of system flexibility, permissibility of remote administration, anomaly detection, compliance with applicable industry standards, for which an IoT product or service was developed.

Keywords: *Internet of things (IoT), compliance control, IT system, information security, protocol.*

ВВЕДЕНИЕ

В настоящее время все больше организаций стремятся перенести бизнес-процессы в цифровую среду, тем самым существенно снижая транзакционные издержки и значительно увеличивая объемы экономической деятельности. Отчасти благодаря безусловным преимуществам возникла и успешно продолжает развиваться концепция сети передачи данных между физическими объектами (или дословно в переводе с англ. «вещами»), которые оснащены встроенными средствами и технологиями для взаимодействия друг с другом или с внешней средой.

Поступила в редакцию 13.05.2022

В этой связи компании, акцентирующие свое внимание на внедрении правил соответствия требованиям безопасности IoT (internet of things), столкнулись в своей практике как минимум с одним инцидентом по информационной безопасности в части применения технологии IoT.

Интеллектуальные системы интернета вещей позволяют быстро производить и оптимизировать новые продукты, а также быстро реагировать на потребности в продуктах. IoT может быть применен для управления активами с помощью прогнозного обслуживания, статистической оценки и измерений для обеспечения максимальной надежности.

С 2020 года внедрение технологии IoT многократно возросло благодаря введению норм социального дистанцирования и изоляции в период пандемии COVID-19. Интенсивность внедрения технологии IoT привела к росту количества обнаружения уязвимостей и нарушений в информационной безопасности IoT.

Согласно исследованиям, проведенными специалистами российских топ-компаний, специализирующимися на информационной безопасности (АО «Лаборатория Касперского»[1], ПАО «Группа Позитив»[2], ПАО «Сбербанк»[3]), в 2020–2021 годах нарушения в подходах к хранению, обработке данных в производственно-технологическом секторе не сократятся, а останутся на том же уровне, что может привести к потенциальной потере миллиардов рублей для этих компаний. Нивелировать риск этих потерь представляется возможным посредством внедрения стандартов (нормативных документов), разработанных в соответствии с требованиями IoT, что позволит решить проблемы информационной безопасности в технологии IoT.

Интернет вещей[4] создает возможности для более прямой интеграции вещей в компьютерные системы, что приводит к повышению эффективности, экономическим выгодам и снижению нагрузки на человека [2].

Так, в июне 2021 г. «СИБУР» впервые вывел комплекс промышленного интернета вещей на рынок внешних продаж. Также компания сделала доступным для внешних заказчиков комплекс дополненной реальности для удаленных консультаций на предприятиях. Ряд российских компаний уже провели успешные тестовые сеансы оборудования на собственных площадках [1].

Необходимо отметить, что выявление текущих или новых комплаенс-рисков, в том числе и в области информационной безопасности при использовании и внедрении технологий IoT, а именно грамотная оценка таких рисков и управление, ответственность за соблюдение нормативных актов (например, Федеральный закон «О персональных данных» от 27.07.2006 №152-ФЗ), а также разработка механизма регулирования событий в компланс-системе внутреннего и внешнего контроля непосредственно входят в обязанности комплаенс-менеджера организации.

СОДЕРЖАНИЕ ИССЛЕДОВАНИЯ И ОСНОВНЫЕ ВЫВОДЫ

В экосистеме IoT[5] есть много составных частей, которые должны соответствовать требованиям для обеспечения общего безопасного информационного взаимодействия. В упрощенном виде можно выделить четыре основные группы, на которые комплаенс-менеджеру необходимо обратить внимание при осуществлении своей деятельности и планировании риск-предотвращающих мероприятий в системе IoT – это люди, процессы, устройства и, безусловно, технологии (в частности программное обеспечение).

Компании, планирующие применять технологии IoT, должны с самого начала знать о существующих IoT-требованиях и о том, каким образом их можно внедрить в свою повседневную деятельность. Данный вопрос, как и все, что связано с корректной организацией процессов в компании, входит в компетенцию комплаенс-менеджера. Бесспорным является тот факт, что если лица, принимающие решения о внедрении технологии IoT, понимают необходимость обеспечения соответствия требованиям безопасности информации и знают или ранее уже имели подобный опыт внедрения, то успех проекту будет обеспечен, а конечный пользователь технологии будет спокоен за сохранность своих данных. Это необходимо для обеспечения соответствия результатов проекта общим бизнес-целям организации. Неспособность выполнить требования по безопасности данных IoT может привести к серьезным утечкам конфиденциальной корпоративной информа-

[1] В 2021 году решения «Лаборатории Касперского» в среднем обнаруживали ежедневно 380 тысяч вредоносных файлов (14 декабря 2021 г.) [Электронный ресурс] (дата обращения 31 марта 2022 г.) URL: https://www.kaspersky.ru/about/press-releases/2021_v-2021-godu-resheniya-laboratorii-kasperskogo-v-srednem-obnaruzhivali-ezhednevno-380-tysyach-vredonosnyh-fajlov.

[2] ПАО «Группа Позитив» аналитическая статья «Кибербезопасность 2020–2021» (28 января 2021 г.) [Электронный ресурс] (дата обращения 01 апреля 2022 г.) URL: https://www.ptsecurity.com/ru-ru/research/analytics/kiberbezopasnost-2020-2021/.

[3] Сбербанк подсчитал потери российской экономики в 2021 году от киберпреступности (18 июня 2020 г.) [Электронный ресурс] (дата обращения 30.03.2022 г.) URL: https://tass.ru/ekonomika/8761953?utm_source=yandex.ru&utm_medium=organic&utm_campaign=yandex.ru&utm_referrer=yandex.ru.

[4] Интернет вещей – сеть физических объектов, обладающих встроенными технологиями взаимодействия с внешней средой с возможностью передачи данных о своём текущем состоянии и приеме данных извне [Электронный ресурс] (дата обращения 30.03.2022 г.) URL: https://www.gartner.com/en/search?keywords=iot.

[5] Экосистема IoT – локальные или глобальные сети устройств, а также компоненты, дающие возможность присоединения к ним новых, обеспечивающие удаленное управление, хранение, передачу и безопасность данных. [Электронный ресурс] (дата обращения 25.03.2022 г.) URL: https://yainvestor.guru/teoriya-finansov/interesnoe/iot.

ции и потерям, которые в лучшем случае будут исчисляться в денежном эквиваленте, в худшем же нанесут сильный удар по репутации компании, а в отдельных случаях могут привести к административной и/или уголовной ответственности.

Одним из ярчайших примеров несоблюдения требований безопасности в использовании IoT-технологий является утечка информации о клиентах сервиса быстрого заказа еды «Яндекс.Еда». Так, 1 марта 2022 г. компания сообщила о том, что в результате недобросовестных действий одного из сотрудников «Яндекс. Еда» в Интернете были опубликованы телефоны клиентов и информация об их заказах: состав, время доставки и иная информация, не подлежащая публичному распространению.

По итогам внутренней проверки Яндекс ужесточил подход к хранению чувствительной информации[6], в том числе связанной с заказами, и планирует обеспечить ей уровень защиты, сопоставимый с уровнем защиты платёжной информации, логинов и паролей. Ручная обработка таких данных будет исключена, а число сотрудников, которые имеют доступ к информации о заказах, сократится как минимум втрое [3].

Однако, несмотря на все заверения руководящего звена сервиса «Яндекс.Еда» об ужесточении контроля за информацией, компании не удастся избежать судебных разбирательств, где за подобную неосмотрительность ей, прежде всего, грозит административная и гражданская ответственность, а также компенсационные выплаты пострадавшим.

Для недопущения подобных вышеописанных ситуаций необходимо уделить пристальное внимание проработке и внедрению на начальной стадии проекта процессов соответствия требованиям IoT.

Первым шагом на пути к комплаенс-контролю IoT должно быть создание процессов для соответствия отраслевым стандартам и протоколам, а также государственным нормативным актам. IoT-системы генерируют огромное количество персональных данных. Правительства во всем мире осознают потенциальный ущерб, вызванный нарушениями безопасности данных, генерируемых системами IoT. Они разрабатывают нормативные рекомендации для компаний, продающих продукты IoT (аппаратное или программное обеспечение).

Например, руководящие принципы безопасности IoT, выпущенные в Великобритании[7] в 2019 г., позволили переложить ответственность за безопасность данных на компанию, продающую продукт IoT. Специфика требований IoT зависит от отрасли, для которой разрабатывается продукт или услуга.

Некоторые отрасли, такие как промышленность, банки и здравоохранение, строго регулируются. Система IoT, работающая в этих направлениях, должна соответствовать всем отраслевым нормативным актам, а также руководящим принципам органов, к которым относятся структуры, осуществляющие подведомственное курирование, например, Министерство здравоохранения, Министерство финансов и т.д. [8].

Широкое внедрение IoT стало возможным в том числе благодаря доступности дешевых устройств и датчиков IoT за последние годы. Однако снижение цен произошло и за счет снижения безопасности. Данный факт обращает наше внимание на проблему, которая заключается в неразрывной связи между аппаратной и программной безопасностью, что является одним из ключевых и необходимых условий успешного использования IoT. Но реализация этого условия не заинтересовала производителей, которые, очевидно, снизили затраты, чтобы сдерживать рост цен на свою продукцию в жестких рыночных условиях конкуренции. Таким образом, ответственность за то, чтобы устройства, используемые клиентами, соответствовали требованиям безопасности IoT, стали нести разработчики соответствующих продуктов IoT.

Экосистема IoT включает устройства IoT, пограничные устройства, сетевую инфраструктуру для подключения и инфраструктуру облачных вычислений. Любой администратор системы IoT должен знать о каждом из устройств и элементов инфраструктуры, составляющих экосистему IoT. Составление полноценного списка всех аппаратных компонентов помогает комплаенс-менеджеру отслеживать, насколько соответствует каждый из них требованиям регуляторов.

Соответствие требованиям для устройств IoT зависит не только от используемой технологии, но и от страны или региона, где она будет использоваться. Например, на территории Российской Федерации любое радиочастотное устройство должно отвечать требованиям Федерального закона от 07.07.2003 №126-ФЗ (ред. от 30.12.2021) «О связи», постановлению Правительства Российской Федерации от 20.10.2021 №1800 «О порядке регистрации радиоэлектронных средств и высокочастотных устройств» и ряду других нормативных правовых актов. Данная сфера деятельности входит в зону контроля Федеральной службы по техническому и экспортному контролю (ФСТЭК России). В США же любое радиочастотное (RF) устройство должно быть разрешено для использования в соответствии с Федеральной комиссией по связям (FCC). Фактически, любое радиочастотное устройство, импортируемое в США, должно соответствовать требованиям FCC. Руководители и контролеры

6 Чувствительная информация – информация, несанкционированное раскрытие, модификация или сокрытие которой может привести к ощутимому убытку или (денежному) ущербу.[Электронный ресурс] (дата обращения 29.03.2022 г.) URL: https://dic.academic.ru/dic.nsf/fin_enc/31656.

7 Code of Practice for Consumer IoT Security [Электронный ресурс] (дата обращения 28.03.2022 г.) URL:https://assets.publishing.service.gov.uk/government/uploads/system/uploads/attachment_data/file/971440/Code_of_Practice_for_Consumer_IoT_Security_October_2018_V2.pdf.

проектов IoT должны обладать знаниями о локализованных требованиях соответствия для используемых устройств IoT.

ИТ-разработчики часто упускают из виду проблемы соответствия требованиям при подключении устройств IoT к сети, хотя это имеет решающее значение для безопасности данных.

В мире уже сейчас разработано множество стандартов, которые могут использоваться при проведении комплаенс-контроля IoT, например:

IEEE 802.11 ah – является частью набора беспроводных протоколов IEEE 802.11. Это низкоэнергетический протокол беспроводной сети для расширения диапазона подключения для сетей Wi-Fi.

Bluetooth low energy – это интеллектуальная и экономичная версия технологии беспроводной персональной сети. Этот протокол используется для приложений в здравоохранении, домашнего применения, фитнесе и системах безопасности.

Zigbee – это беспроводной протокол на основе IEEE 802.3 15.4 для устройств с низким энергопотреблением и низкой пропускной способностью, используемых в устройствах, которые являются частью медицинских, домашних или персональных сетей.

Z-wave – это беспроводной сетевой протокол с низким энергопотреблением, разработанный для систем домашней автоматизации.

В идеале эти протоколы должны быть встроены в качестве встроенного программного обеспечения (далее – ПО) в устройства IoT, в таком случае комплаенс-контроль IoT сводится к правильному выбору устройств. Но не все так просто. Многие устройства не имеют встроенных в них необходимых протоколов. Команда разработчиков системы IoT несет ответственность за обеспечение соответствия в выбранных ими устройствах.

Защита информационных систем и связанных с ними данных имеет важное значение при осуществлении комплаенс-контроля. Эти данные могут быть сгенерированы как самой системой, так и использоваться для ее поддержания и корректного функционирования и выполнения предустановленного перечня задач. Независимо от типа все данные должны быть защищены. Небезопасные устройства IoT представляют серьезную угрозу для модели информационной защищенности Федеральных служб (Федеральная служба безопасности, Федеральная таможенная служба, Федеральная служба по контролю за оборотом наркотиков, и т.д.) поскольку они могут выступать в качестве уязвимого шлюза для всей информационной системы. Независимо от того, находятся ли устройства IoT в самой организации или установлены на сайте клиента, все они подключаются к общей сети, которая может быть легко скомпрометирована, если какое-либо из устройств IoT небезопасно.

Фактически, умная лампочка или камера, подключенные к Интернету, могут стать лазейкой для хакеров, ищущих способы взлома сети. Компании, инвестировавшие в обеспечение соответствия требованиям IoT, должны знать о трех наиболее важных компонентах информационной безопасности, которые не должны компрометировать систему IoT:

1. Конфиденциальность – набор правил, которые гарантируют, что доступ к информации получают только уполномоченные люди. Данные, как правило, классифицируются в соответствии с их уровнем доступности. Далее меры конфиденциальности реализуются в соответствии с важностью этих уровней.

К примеру, шифрование, пароли, двухфакторная аутентификация и биометрическая проверка являются одними из наиболее часто используемых методов поддержания конфиденциальности данных. Аппаратные меры безопасности, такие как использование компьютеров с воздушным зазором или отключенных устройств хранения данных, также могут использоваться, если данные очень критичны и имеют заведомо сомнительный характер.

2. Целостность – гарантирует, что согласованные, точные и надежные данные сохраняются на протяжении всего жизненного цикла. Данные не должны изменяться во время передачи или хранения. Первым шагом в обеспечении целостности данных является ограничение доступа, т.е. доступ для внесения изменений должен быть предоставлен только уполномоченным лицам, каждый пользователь не должен иметь возможность устанавливать обновления.

Права доступа к файлам, контроль доступа пользователей, контрольная сумма и резервные копии – это лишь некоторые из способов поддержания целостности данных. Периодические резервные копии необходимы для восстановления данных, которые были изменены неосознанно или потеряны в результате атаки киберпреступников.

3. Доступность – подразумевает под собой, что правильные данные должны быть доступны авторизованным пользователям по мере необходимости. Это стало возможным благодаря поддержанию и обновлению всей аппаратной инфраструктуры. Аппаратное и программное обеспечение должны быть обновлены, когда это необходимо.

Поддержание требуемой пропускной способности и предотвращение узких мест в сети является важным аспектом доступности 24/7. Необходимо хранить несколько резервных копий данных, чтобы в случае сбоя одного сервера другой был готов выполнить требования пользователей [4].

Следующим немаловажным вопросом при проведении комплаенс-контроля является изучение инцидентов безопасности с технологиями IoT, с которыми сталкивается любая организация и которые зависят от доступа организации к экспертным знаниям в области

безопасности IoT. Количество инцидентов в информационной безопасности обратно пропорционально опыту в области безопасности IoT.

В настоящий момент можно выделить три уровня пользователей, имеющих тот или иной опыт в обеспечении информационной безопасности IoT.

Высший уровень – компании, имеющие достаточно малое количество проблем безопасности с IoT в связи с приобретенным опытом в решении конкретных инцидентов по информационной безопасности IoT.

Средний уровень – компании, имеющие проблемы, но также демонстрирующие наличие определенной степени опыта в успешном внедрении безопасности IoT.

Нижний уровень – компании, сталкивающиеся с большим количеством проблем из-за отсутствия опыта в области безопасности IoT.

Интересным является тот факт, что проблемы безопасности IoT, с которыми сталкиваются компании верхнего и нижнего уровней, заметно различаются (табл. 1).

Для обеспечения соответствия требованиям IoT комплаенс-менеджеру самому и/или при помощи лиц, ответственных за конкретные процессы в организации (например, сотрудники ИТ-службы, и т.п.), необходимо последовательно выполнить четыре основных шага:

1) создать контрольный список соответствия требованиям;

2) провести анализ рисков, учитывая специфику среды, в которой будет работать продукт или услуга IoT;

3) провести тесты, чтобы убедиться, что все пункты в контрольном списке требований выполнены;

ТАБЛИЦА 1.
Проблемы безопасности IoT

Предприятия высшего уровня	Предприятия нижнего уровня
Шифрование конфиденциальных данных	Денежный ущерб
Обеспечение целостности данных во время передачи данных	Потеря производительности
Масштабирование мер безопасности	Юридические / штрафы за соблюдение требований
Обеспечение доставки обновлений	Потерянная репутация
Обеспечение безопасности хранения ключей шифрования на основе программного обеспечения	Снижение цен на акции

Источник: составлено авторами.

4) проводить плановые или внеплановые проверки информационной системы на предмет перманентного соответствия и актуальности требованиям IoT.

Помимо вышеуказанных этапов, представляется необходимым на постоянной основе выполнять следующие рекомендации:

1. Срок годности продукта или устройства. Каждый продукт или устройство имеет срок годности, который в идеале должен быть указан во время его запуска. Необходимо позаботиться о том, чтобы регулярно проводились работы по обновлению ПО или замене аппаратных частей системы IoT. Обеспечение требований комплаенс-контроля в части безопасности информации в системах IoT может оказаться более дорогостоящим для продуктов или устройств с истекшим сроком службы.

2. Авторизация и аутентификация – разрешение на доступ или обновление данных в устройствах должно предоставляться только тем, кто непосредственно попадает в зону ответственности за изменение затрагиваемых процессов. Это становится особенно важным в многопользовательских продуктах для отслеживания инцидентов безопасности.

3. Защита данных – на этапе проектирования необходимо принять решение о том, какой тип данных должен генерироваться системой IoT и как они должны храниться. Сбор ненужной информации увеличивает риск компрометации данных и ведет к дополнительным расходам.

4. Комплексное тестирование – продукты и устройства IoT должны быть тщательно протестированы на все перечисленные риски безопасности, а также на все протоколы и рекомендации, которых необходимо придерживаться. В зависимости от системы IoT и ее архитектуры может потребоваться включить соблюдение дополнительных руководящих принципов государственных или отраслевых органов.

5. Важно обеспечить гибкость системы, чтобы структура IoT допускала возможность включения новых инструментов и руководящих принципов.

6. Обеспечение удаленного администрирования. Так как отзыв продуктов или услуг является дорогостоящим мероприятием, то эти продукты или услуги должны быть разработаны таким образом, чтобы обеспечить удаленную настройку в случае возникновения каких-либо проблем.

7. Обнаружение аномалий – платформа IoT должна быть способна идентифицировать необычные паттерны (образец, шаблон, повторяющийся фрагмент и т.п.) в данных или необычное поведение устройств, чтобы их можно было вовремя обнаружить и устранить угрозу.

8. Отраслевое соответствие – некоторые отрасли имеют строгие руководящие принципы. Данные принципы должны быть частью контрольного списка соответствия.

Системы IoT должны проверяться так же, как и любая ИТ-система. Комплаенс-менеджерам в своей деятельности необходимо использовать стандартизированную процедуру для организации комплаенс-контроля, который в свою очередь должен гарантировать соблюдение законных, финансовых, налоговых, лицензионных, регламентных и т.п. требований во избежание претензий государственных органов и контрагентов, а также любого вида рисков.

ЗАКЛЮЧЕНИЕ

Все компании, которые пытаются внедрить соответствия требованиям безопасности IoT, сталкивались по крайней мере с одним из многих рисков при использовании системы IoT. Чтобы уменьшить вероятность возникновения таких рисков, крайне важно внедрить комплаенс-контроль IoT в организации. Люди, процессы, устройства, технологии и приложения, составляющие экосистему IoT, должны соответствовать требованиям информационной безопасности. В каждой компании, использующей IoT, должен быть хотя бы один сотрудник, ответственный за соблюдение данных требований.

Защита систем Интернета вещей имеет решающее значение, поскольку сами устройства (серверы, компьютеры, смартфоны и т.д.) могут оказаться слабым шлюзом для целых сетей. Системы Интернета вещей не должны ставить под угрозу конфиденциальность, целостность и доступность информационных систем. Чтобы обеспечить соответствие требованиям, первым шагом необходим глубокий анализ продукта или услуги на предмет рисков. После того, как пилотная версия продукта или услуги готова, следует на обязательной основе провести тесты, чтобы убедиться, что контрольный список соответствия соблюдается.

Для обеспечения постоянного соответствия необходимо проводить периодические аудиты. У каждого продукта или устройства есть срок годности. Необходимо внедрить протоколы авторизации, аутентификации, защиты данных, комплексного тестирования. Платформа IoT должна быть способна идентифицировать необычные паттерны в данных или необычное поведение устройств, чтобы потенциальные вторжения могли быть вовремя обнаружены. Продукт или услуга также должны быть разработаны для удаленной настройки, чтобы будущие обновления могли быть сделаны без необходимости отзыва такого продукта или услуги. Системы IoT должны быть настроены и соответствовать требованиям по информационной безопасности так же, как и любая IT-система.

Литература

1. **Лагутенков А.** Тихая экспансия интернета вещей // Наука и жизнь. 2018. № 5. С. 38–42.
2. Постановление Правительства Российской Федерации от 20.10.2021 №1800 «О порядке регистрации радиоэлектронных средств и высокочастотных устройств» [Электронный ресурс] (дата обращения 28.03.2022) URL:http://ivo.garant.ru/#/document/402961872/paragraph/1/doclist/6647/showentries/0/highlight/Постановление%20Правительства%20РФ%20от%2020%20октября%202021%C2%A0г.%20N%C2%A01800%20%20О%20порядке%20регистрации%20радиоэлектронных%20средств%20и%20высокочастотных%20устройств:2.
3. Промышленный интернет вещей (2020) [Электронный ресурс] (дата обращения 02.04.2022) URL: https://investmoscow.ru/media/3340535/03-промышленный-интернет-вещей.pdf.
4. СИБУР развивает разработки для импортозамещения в области промышленного интернета вещей (01 апреля 2022) [Электронный ресурс] (дата обращения 02.04.2022) URL: https://www.cnews.ru/news/line/2022-04-01_sibur_razvivaet_razrabotki.
5. Служба безопасности Яндекс Еды сообщила об утечке информации (01 марта 2022) [Электронный ресурс] (дата обращения 01.04.2022). URL: https://yandex.ru/company/services_news/2022/01-03-2022.
6. Умное будущее. www.kommersant.ru (29 марта 2017) [Электронный ресурс] (дата обращения: 01 апреля 2022). URL: https://www.kommersant.ru/doc/3256300.
7. Федеральный закон от 07.07.2003 №126-ФЗ «О связи» (ред. от 30.12.2021) [Электронный ресурс] (дата обращения 02.04.2022) URL: https://base.garant.ru/186117.
8. **Calatayud A.** The Connected Supply Chain: Enhancing Risk Management in a Changing World. Inter-American Development Bank, 2017. (03).

References

1. **Lagutenkov A.** Silent expansion of the Internet of things. *Nauka i zhizn'*. 2018; (5):38–42. (In Russian).
2. Decree of the Government of the Russian Federation of October 20, 2021 N 1800 «On the procedure for registering radio electronic equipment and high-frequency devices». Electronic resource (accessed on March 28, 2022) URL:http://ivo.garant.ru/#/document/402961872/paragraph/1/doclist/6647/showentries/0/highlight/. (In Russian).
3. Industrial Internet of Things (2020) Electronic resource (accessed 04/02/2022) URL: https://investmoscow.ru/media/3340535/03-industrial-Internet-of-Things.pdf. (In Russian).
4. SIBUR develops developments for import substitution in the field of industrial Internet of things (April 01, 2022) Electronic resource (accessed 04/02/2022) URL: https://www.cnews.ru/news/line/2022-04-01_sibur_razvivaet_razrabotki. (In Russian).
5. The Yandex Food security service reported an information leak (March 01, 2022) Electronic resource (ac-

cessed 04/01/2022). URL: https://yandex.ru/company/services_news/2022/01-03-2022. (In Russian).

6. Smart future. www.kommersant.ru (March 29, 2017) Electronic resource (date of access: April 01, 2022). URL: https://www.kommersant.ru/doc/3256300. (In Russian).
7. Federal Law of July 7, 2003 N 126-FZ «On Communications» (as amended on December 30, 2021) Electronic resource (accessed on April 2, 2022) URL: https://base.garant.ru/186117/. (In Russian).
8. **Calatayud A.** The Connected Supply Chain: Enhancing Risk Management in a Changing World. Inter-American Development Bank, 2017. (03).

Иванченко Надежда Шавкатовна,
старший преподаватель кафедры «Комплаенс и контроллинг» Высшей школы промышленной политики и предпринимательства, РУДН

117198, г. Москва, ул. Миклухо-Маклая, 6
117198, Moscow, st. Miklukho-Maclay, 6
тел: +7 (495) 787-38-03, E mail: 777-333-777@mail.ru

Лепешкин Дмитрий Сергеевич,
студент 1 курса магистратуры кафедры «Комплаенс и контроллинг» Высшей школы промышленной политики и предпринимательства, РУДН

117198, г. Москва, ул. Миклухо-Маклая, 6
117198, Moscow, st. Miklukho-Maclay, 6
тел: +7 (495) 787-38-03, e-mail: Devo84@mail.ru

Кульгускина Мария Александровна,
студентка 1 курса магистратуры кафедры «Комплаенс и контроллинг» Высшей школы промышленной политики и предпринимательства, РУДН

117198, г. Москва, ул. Миклухо-Маклая, 6
117198, Moscow, st. Miklukho-Maclay, 6
тел: +7 (495) 787-38-03, e-mail: bcdfdcb@yandex.ru

Гиниятуллин Аяз Фирдависович,
аспирант Института региональных экономических исследований

119002, г. Москва, пер. Сивцев Вражек, д. 29/16
119002, Moscow, per. Sivtsev Vrazhek, 29/16
тел.: +7 (499) 241-04-18, e-mail: 1576gaf@mail.ru