УДК 34.096 **DOI: 10.34670/AR.2024.95.70.051**

Развитие Интернета вещей и проблемы обеспечения его безопасности

Акапьев Виктор Львович

Кандидат педагогических наук,
доцент кафедры информационно-компьютерных технологий
в деятельности ОВД,
Белгородский юридический институт МВД России им. И.Д. Путилина,
308024, Российская Федерация, Белгород, ул. Горького, 71;
e-mail: nazhukova2008@yandex.ru

Савотченко Сергей Евгеньевич

Доктор физико-математических наук, доцент,
профессор кафедры математики,
Российский государственный геологоразведочный университет
им. Серго Орджоникидзе,
117485, Российская Федерация, Москва, ул. Миклухо-Маклая, 23;
e-mail: nazhukova2008@yandex.ru

Жукова Наталья Алексеевна

Кандидат юридических наук, доцент,
заведующий кафедрой судебной экспертизы и криминалистики,
Белгородский государственный национальный
исследовательский университет,
308015, Российская Федерация, Белгород, ул. Победы, 85;
e-mail: nazhukova2008@yandex.ru

Аннотация

Широкомасштабное внедрение Интернета вещей требует от законодателя совершенствования правового обеспечения информационной безопасности личности и глобального переосмысления юристами процесса становления информационного общества. Объектом исследования стали уязвимости Интернета вещей в контексте обеспечения информационной безопасности профессиональной деятельности на фоне повсеместного и динамично развивающегося использования компьютерной техники, информационных технологий и средств коммуникации, пересечения с пространством IoT критической информационной инфраструктуры Российской Федерации.

Для цитирования в научных исследованиях

Акапьев В.Л., Савотченко С.Е., Жукова Н.А. Развитие Интернета вещей и проблемы обеспечения его безопасности // Вопросы российского и международного права. 2024. Том 14. № 2А. С. 257-267. DOI: 10.34670/AR.2024.95.70.051

Ключевые слова

Базовые принципы IoT, защита информации, интернет вещей, информационная система, кибербезопасность, операционные технологии, технологии IoT, требования к системам IoT, уязвимости IoT.

Введение

Глобальная сеть позволяет вести мониторинг транспорта, всевозможных товаров, осуществлять почти автономное строительство и многое другое. По данным исследований, в 2020 году самый высокий уровень проникновения информационных технологий наблюдался в транспорте, энергетике, ритейле, управлении жизнью города, здравоохранении и промышленности [Коммуникационные технологии Интернета вещей. Что это такое, www].

Глобальная сеть является фундаментом, на который опирается информационная технология под названием «Интернет вещей», которая по своей сути представляет собой процесс объединения мелких сетей в крупные и, наконец, в одну глобальную мировую сеть, где реализуется тесная интеграция виртуального и реального миров, обеспечивающая общение между людьми и устройствами [Что такое интернет вещей и как он устроен, www].

Интернет вещей все активнее входит в нашу жизнь: умные часы, умный чайник и др. Даже умный дом. Но, оказывается, и это не предел. В настоящее время Интернет вещей может существовать и без Интернета. В тех же проездных билетах есть радиомодуль, но отсутствует интернет-протокол.

Технология Интернета вещей может быть использована для автоматизации процесса производства, управления логистикой и движением продукции, осуществления дистанционного мониторинга состояния удаленных объектов (телеметрия, видеонаблюдение, контроль доступа, диагностика состояния технических систем).

Основная часть

В настоящее время специалисты выделяют уже четыре уровня Интернета вещей. Каждый из них является частью следующего:

BAN – все, что находится на человеке: умные часы, кроссовки, футболки, очки и т.д.;

LAN – по сути это умный дом, т.е. различные устройства, объединенные в одну сеть;

WAN – умные города, общественный транспорт, объединенный в одну сеть и имеющий выход в Интернет, электростанции, автоматически перераспределяющие нагрузку и т.д.;

VWAN – умная планета, где каждое устройство может взаимодействовать с любым другим [Актуальность проблемы обеспечения безопасности информации, www].

Если с первым и вторым уровнями все понятно, то третий и четвертый пока выглядят как утопия. Но это пока. Двадцать лет назад никто не мог предсказать, что будет с Интернетом, а он везде. Тоже следует ожидать и с автоматизацией всех областей человеческой деятельности.

Противники такого подхода ссылаются на угрозы, которые несет рассматриваемая технология. Одна из них – слежка. Уже сейчас браузер записывает буквально каждый шаг пользователя в сети и атакует контекстной рекламой. В будущем крупные компании будут знать весь ваш распорядок дня, чем вы интересуетесь, что вы едите, как долго спите и куда идете.

При использовании облачных сервисов для реализации Интернета вещей могут возникнуть

проблемы с доступом, и, что значительно важнее, вы не являетесь хозяином своих данных, поскольку все ваши данные сливаются на облачный сервер и повлиять на решение компании, владеющей этим сервисом, вы уже не можете. Фактически пользователь передает свои данные в доверительное управление не совсем понятно кому. Таким образом, эти данные могут быть не только просто перехвачены, но и физически уничтожены.

Возникает правовой парадокс: приобретая какой-нибудь товар в Интернете вещей, вы не становитесь его собственником, вы его арендуете. Примером может служить изменение наименования «иконок» на рабочем столе операционной системы Windows. Если раньше использовалось название «Мой компьютер», то в новых версиях этот значок обозначается как «Компьютер» или «Этот компьютер».

Но самый распространенный страх – это страх взлома устройств. Для одного бытового гаджета это не так страшно, но атаки на коммунальные системы, предприятия промышленного производства, базы и банки данных государственных министерств и ведомств могут обернуться глобальной катастрофой.

В 2008 году национальная разведка США назвала технологию Интернета вещей разрушительной и причислила к главным мировым угрозам информационной безопасности [Шиков, 2017, 29].

С Интернетом вещей связана и другая проблема – киберпреступность. Подключение всего и вся к Интернету открыло для киберпреступников сказочные возможности. В 2016 году мир узнал о первом в истории виртуальном угоне: хакеры получили доступ к управлению автомобилем, когда за рулем был водитель, и просто остановили его [Езда по воле хакера, www].

Приведем наиболее известные примеры успешных кибератак на IoT.

В 2016 году сотни тысяч скомпрометированных сетевых устройств были вовлечены в ботнет Mirai, который превратил их в прокси-серверы для вредоносного трафика.

В 2018 году вредоносная программа VPNFilter заразила более полумиллиона маршрутизаторов, установив на устройства IoT вредоносное ПО, которое перехватывает трафик и крадет пароли [Вирус VPNFilter: описание, возможности, список уязвимых устройств, www].

В 2018 году через умный термометр декоративного аквариума в фойе хакеры смогли проникнуть в локальную сеть казино и скопировать базу данных хайроллеров (VIP-игроков на высоких ставках), представляющую коммерческую тайну [Казино взломали через термостат в аквариуме, www].

Впрочем, вопрос, как предотвращать подобные ситуации в будущем, так и остался открытым. Но переход к Интернету вещей в том или ином виде уже идет. Количество «умных» устройств, подключенных к сети, уже сегодня в три раза превышает население Земли, и в будущем их число будет только увеличиваться [Тенденции технологии IoT в 2023 году, www].

Разработка алгоритмов взаимодействия и внедрения в новые сферы – только вопрос времени, поэтому актуализируется необходимость решения проблемы уязвимости Интернета вещей с точки зрения кибербезопасности.

Кибербезопасность относится к числу направлений деятельности, развивающихся чрезвычайно быстрыми темпами. Этому способствуют как общий прогресс развития информационных технологий, так и постоянное противоборство различных сторон в процессе сохранности и приобретения информации. Поэтому проблемы, связанные с кибербезопасностью, с каждым годом становятся все более насущными и сложными.

Широкое внедрение информационные технологии получили и в деятельности государственных органов. Огромный объем аккумулируемой информации (открытой,

конфиденциальной, служебной, персональных данных, государственной тайны) ставит нормальное функционирование государственных структур в зависимость от различного рода информационных угроз. При этом защитные меры оказываются значительно более дешевыми и эффективными в случае, если они встроены в информационные системы и сервисы на стадиях задания требований и проектирования.

Когда данный момент упущен и информационная система уже находится в эксплуатации, необходимо понимать, что зачастую реальная стоимость информации, циркулирующей в системе, может в разы превышать стоимость самой системы, поэтому актуализируется необходимость защиты информации в составе информационных систем.

Помимо всего прочего, на передний план борьбы за обеспечение информационной безопасности выходят следующие мотивирующие основания:

– обостряющиеся противоречия между все возрастающими потребностями общества в свободном обмене информацией и ограничениями (чрезмерным или, наоборот, недостаточным) на её распространение и использование;
– повсеместное и динамично развивающееся использование компьютерной техники, информационных технологий и средств коммуникации;
– использование информационных систем в критических областях деятельности;
– консолидация в рамках единого информационного пространства все большего числа граждан и организаций;
– концентрация огромных объёмов жизненно важной информации различного назначения и принадлежности на электронных носителях;
– количественное и качественное совершенствование способов доступа пользователей к информационным ресурсам;
– превалирование доли информационных услуг в формировании валового национального продукта ведущих стран мира, создание и развитие цифровой экономики, цифровой энергетики и др.;
– превращение информации в товар и переход к рыночным отношениям в области предоставления информационных услуг;
– расширение многообразия видов угроз и возникновение новых возможных каналов утечки информации;
– рост числа квалифицированных пользователей современных информационных технологий, обладающих достаточно сформированной информационно-технологической компетентностью, позволяющей им создавать нежелательные воздействия на системы обработки информации;
– увеличение ущерба от уничтожения, фальсификации, разглашения или незаконного тиражирования информации [Портал iot.ru «Новости Интернета вещей», www].

Несмотря на существенные изменения законодательства в последние годы в сфере информационной безопасности и защиты информации от противоправных действий, проблемы не ликвидированы полностью. Существуют противоправные действия, по которым отсутствует понятийная база, что позволяет преступникам уходить от уголовного преследования. Используются методы социальной инженерии, которые выводят преступника из-под преследования, создавая ситуации якобы добровольной передачи денег, материальных ценностей или информации.

Отсутствие стройной и непротиворечивой системы законодательно-правового

регулирования отношений в сфере оборота и защиты информации создаёт условия для возникновения и широкого распространения «компьютерного хулиганства» и «компьютерной преступности» [Рогачева, 2021, 558].

Возрастает количество противоправных действий, совершаемых преступными группами по заранее составленному плану и соответствующему алгоритму. Это деятельность мошенников по получению доступа к банковским картам населения, принявшая в последние годы массовый характер. Шифрование информационных ресурсов, взлом сайтов и серверов с последующим вымогательством денежных средств. Также в составе преступных групп осуществляются попытки доступа к информационным ресурсам государственных органов, промышленный шпионаж. Существенная часть противоправных действий осуществляется под кураторством или непосредственным руководством иностранных разведок. В ряде иностранных государств, таких как США, Великобритания, Украина, созданы специализированные подразделения для проведения противоправных действий в информационном пространстве других стран и, в первую очередь, России.

В эпоху всеобщей цифровизации пространство Интернета захватывает новая информационно-коммуникационная технология – Интернет вещей, где информационные процессы проходят практически без участия человека. В отличие от Интернета людей, в Интернете вещей ведущую роль играют программно-аппаратные комплексы, способные взаимодействовать друг с другом и с управляющим сетевым ПО.

Конечная точка – это однозначно идентифицируемое в сетевом пространстве устройство, способное самостоятельно обрабатывать данные для взаимодействия с человеком, с другими устройствами или с внешней физической средой.

В Интернете вещей сетевыми конечными точками являются сенсоры, сервоприводы, контроллеры производственных операций; бытовые приборы; датчики систем пожарной и охранной сигнализации; камеры систем компьютерного зрения; point-of-sale терминалы; компоненты систем искусственного интеллекта и т.п.

Интернет вещей – инфраструктура взаимосвязанных сущностей, АИС и ИР, а также служб, позволяющих обрабатывать информацию о физическом и виртуальном мире и реагировать на нее.

Технические устройства для сбора данных – сенсоры или датчики. Датчики собирают данные, преобразуют их в сигнал и отправляют сигнал платформе.

Шлюз IoT – сетевое устройство, предназначенное для передачи данных между устройствами IoT и сетью Интернет.

Концепция IoT предполагает тесную взаимосвязь между информационными технологиями и операционными технологиями.

Операционные технологии – это процессы, методы и средства управления в *киберфизических системах*, где вычислительные ресурсы интегрированы с физическими сущностями любого вида, включая биологические и рукотворные объекты.

Технологии IoT используются в различных отраслях: производство, автомобилестроение, здравоохранение, транспорт, логистика, энергетика, сельское хозяйство и др. В зависимости от целей конкретной системы IoT интеллектуальные устройства могут варьироваться от простых датчиков освещенности до оборудования для анализа ДНК. Все чаще вокруг встречаются технологии умного дома, умного города, бодинет.

На абстрактном уровне IoT можно сравнить с информационной моделью человека. Тело собирает информацию об окружающей среде через сенсоры – органы чувств (зрение, слух,

осязание, обоняние, вкус). Мозг осмысливает поступающие данные, сравнивает с известными образами в своей базе знаний и принимает решение по управлению частями тела. Если принятые образы отсутствуют в базе знаний, то мозг пытается их осознать, пользуясь накопленным опытом и правилами логики, и включить в базу знаний. В 2018 году в сферах транспорта, производства, систем автоматизации и других платформ корпоративного класса во всем мире использовалось около 8 млрд устройств («точек») IoT, в 2020 году их было около 12 млрд, к 2025 году, по разным прогнозам, подключенных устройств будет 25 млрд или почти 60 млрд [Интернет вещей, www]

Базовые принципы IoT:

распределенная сетевая инфраструктура, позволяющая доставлять данные в конечные точки IoT по оптимальным маршрутам;

уникальный идентификатор для любого устройства IoT;

наличие пользовательского интерфейса для ручного управления устройствами IoT;

гарантированная доступность каждого устройства IoT и возможность коммуникации с управляющим ПО или пользователем в режиме реального времени;

экономическая эффективность.

По сути, IoT – это новая концепция информационно-телекоммуникационных сети, объединяющей на основе архитектуры Интернет множество датчиков и исполнительных устройств для управления технологическими процессами в автоматическом режиме с минимальным участием человека. При этом требования к архитектуре, надежности и функциональным возможностям IoT в некоторых случаях выходят за рамки Интернета людей.

С точки зрения информационной безопасности архитектура IoT подразделяется на несколько уровней.

Физический уровень (уровень вещей) представляет два типа операций – сбор информации (датчики) и механические действия (актуаторы, исполнительные механизмы).

На физическом уровне функционируют относительно простые датчики (световые, звуковые, емкостные, индуктивные, электрические, концевые выключатели, измерители угла поворота, скорости вращения и т.п.) и сложные сенсоры-анализаторы (спектра, химического состава, компьютерное зрение), собирающие данные в реальном времени.

Актуаторы IoT – это, как правило, электронные ключи и контроллеры различных механизмов и технических систем.

Примерные требования к устройствам IoT различного применения: минимальная цена; надежность, защищенность от климатических воздействий; низкое энергопотребление и автономное электропитание; минимальные затраты на установку и обслуживание; машинное обучение; для видеокамер – первичная обработка изображения с принятием решения на основе искусственного интеллекта и т.п.

Как видно из примера, в некоторых случаях требования могут быть противоречивыми.

Сетевой уровень обеспечивает обмен данными «вещей» с управляющим ПО.

Некоторые системы IoT предполагают размещение устройств и управляющего ПО в одной сети или прямое подключение через сотовую связь, но чаще устройства IoT подключаются к управляющим приложениям в сети Интернет через шлюзы (gateway), которые выступают в роли агрегаторов исходных данных и маршрутизаторов пакетов.

Прикладной уровень представляет набор служб и приложений, обеспечивающих автоматизацию бизнес-процессов в IoT.

В последнее время возникли дополнительные требования к системам IoT: данные имеют

неограниченный объем; данные являются разнородными (количественными, качественными, текстовыми); результаты должны быть конкретны и понятны; инструменты для обработки сырых данных должны быть просты в использовании; методы традиционной математической статистики не подходят для анализа и прогнозирования поведения систем.

В этой связи интеллектуальные возможности IoT расширяются за счет технологий анализа больших данных, в том числе глубинного, а также машинного обучения.

В качестве наглядного примера можно рассмотреть популярную концепцию «умного дома» с автоматическим управлением его инженерной инфраструктурой.

Глобальная задача Интернета вещей заключается в том, чтобы взять на себя управление огромными по объему данными, оставив человеку контрольные функции. Это подразумевает не просто обмен сигналами, а генерацию управляющих советов для людей [Nozari, Fallah, Kazemipoor, Najafi, 2021, 80].

Главная сложность сейчас заключается в том, чтобы научиться доверять Интернету вещей. Уход от отработанных алгоритмов формальной логики и методов компьютерно-математического моделирования создает барьер в доверии к данной технологии.

Другой барьер касается кибербезопасности: из-за того, что данные становятся глобальными, из-за того, что в эту сферу вовлекается все большее количество людей и организаций, которые ревностно стараются оберегать свои данные, происходит обратный эффект – далеко не все готовы делиться с другими своей информацией.

Корректное функционирование технологии Интернета вещей опирается на неукоснительную реализацию следующих принципов: конфиденциальность информации; доступность информации; целостность информации.

Нарушение любого из перечисленных принципов приводит к возможности негативных последствий для пользователя IoT, а основной причиной является недостаточный уровень обеспечения информационной безопасности IoT, которая подразумевает защиту устройств и сетей, к которым они подключены, от сетевых атак и взломов.

Повышение данного уровня достигается путем выявления, мониторинга и устранения потенциальных уязвимостей безопасности IoT, к которым относятся ненадежные или несменяемые пароли доступа к устройствам IoT; сохранение заводских (общеизвестных) паролей; сквозная авторизация – для взлома сети достаточно взломать одно устройство; отсутствие шифрования сетевого трафика; использование небезопасного ПО и протоколов сетевого обмена; наличие потенциально опасных сетевых сервисов и открытых портов; небезопасные настройки по умолчанию и ограниченное управление устройством; отсутствие технической поддержки и безопасных механизмов обновления ПО; отсутствие средств защиты от сетевых атак и вредоносного ПО; возможность физического доступа к устройству посторонних; типовые уязвимости мобильных технологий и облачной инфраструктуры.

Требования к кибербезопасности индустриального IoT устанавливаются государством или эксплуатирующими организациями, исходя из оценки рисков. В значительной степени с пространством IoT пересекается критическая информационная инфраструктура Российской Федерации, но государство по каким-то причинам не обращает серьезного внимания на нарастающую проблемную ситуацию.

В настоящее время основная с точки зрения информационной безопасности проблема IoT заключается в следующем: нередко заказчики и разработчики думают о безопасности в последнюю очередь: сначала разработка и внедрение продукта, затем безопасность. Необходимо сразу разрабатывать структуру так, чтобы она была безопасной, важно

взаимодействие команды разработки IoT и команды ИБ на всех этапах, анализ угроз на этапе разработки и применение необходимых средств, как встроенных, так и дополнительных.

Подход к защите разделяется на две части: защита от устройств; защита самого IoT.

Перечень мер защиты IoT должен включать следующие элементы: физическая безопасность; доверенная загрузка; безопасная операционная система; защита на уровне приложений; управление учетными записями; шифрование; безопасность каналов связи; контроль взаимодействия; обновление программного обеспечения, прошивок; проведение аудита.

Заключение

Безопасность Интернета вещей принципиально не отличается от международного стандарта ISO27001 [ISO/IEC 27001 Системы менеджмента информационной безопасности, www], но необходимо создавать отдельный раздел этого стандарта, ориентированного именно на обеспечение безопасности технологии IoT. В нем должны быть указаны следующие элементы защиты информации в сфере Интернета вещей: все компоненты системы IoT, как технические, так и информационные, должны быть учтены, должна быть реализована точная идентификация и классификация всех IoT устройств; безопасность должна быть приоритетом при создании IoT не зависимо от ее масштаба; безопасность следует учитывать на этапе проектирования, чтобы лучше ее интегрировать во все аспекты системы; каждое устройство, подключаемое к сети, должно быть настроено с точки зрения обеспечения безопасности; обнаружение аномалий и уязвимостей; применение политик безопасности на основе информации об IoT устройствах; стратегия безопасности организации должна строиться на допущении компромисса: защита устройств, безусловно, важна, но нет абсолютной защиты; корпоративная сеть должна быть защищена от самих устройств IoT, которые несут угрозу.

Размытие границы между технической и личной информацией актуализирует развитие правовой составляющей обеспечения информационной безопасности, ориентированной не только на регламентацию принципов сбора и обработки информации, но и, в первую очередь, на защиту персональных данных.

В целом, регулирование IoT не требует создания специального законодательства, а соответствующие нормы могут быть включены в существующие нормативно-правовые акты.

Библиография

1. Актуальность проблемы обеспечения безопасности информации. URL: https://searchinform.ru/informatsionnaya-bezopasnost/osnovy-ib/osnovnye-aspekty-informatsionnoj-bezopasnosti/osnovnye-printsipy-obespecheniya-informatsionnoj-bezopasnosti/problemy-obespecheniya-bezopasnosti-informatsii.
2. Верещагина Е.А., Капецкий И.О., Ярмонов А.С. Проблемы безопасности Интернета вещей. М.: Мир науки, 2021. URL: https://izd-mn.com/PDF/20MNNPU21.pdf.
3. Вирус VPNFilter: описание, возможности, список уязвимых устройств. URL: https://networkguru.ru/virus-vpnfilter-opisanie-vozmozhnosti-ustroystva.
4. Езда по воле хакера. URL: https://www.kommersant.ru/doc/2773532.
5. Интернет вещей. URL: https://sber.pro/digital/education/internet_vesshei.
6. Информационная безопасность автоматизированных систем: понятие, методы обеспечения. URL: https://gb.ru/blog/informatsionnaya-bezopasnost-avtomatizirovannykh-sistem.
7. Казино взломали через термостат в аквариуме. URL: https://habr.com/ru/companies/globalsign/articles/354256.
8. Коммуникационные технологии интернета вещей. Что это такое. URL: https://tulasprav.ru/articles/kommunikatsionnye-tehnologii-interneta-veschey-chto-eto-takoe.html.
9. Пиковер А.В. Интернет вещей и промышленный интернет вещей в КНР // Сборник статей ежегодной научной

конференции Центра экономических и социальных исследований Китая Института Дальнего Востока РАН «Социально-экономические итоги 13-й пятилетки КНР (2016-2020 гг.) и задачи 14-й пятилетки (2021-2025 гг.)». М., 2021. С. 195-209.
10. Портал iot.ru «Новости Интернета вещей». URL: https://iot.ru.
11. Рогачева Н.В. Интернет вещей: обзор основных проблем и задач // Languages in professional communication. 2021. С. 558-563.
12. Суомалайнен А. Интернет вещей: видео, аудио, коммутация. М.: ДМК Пресс, 2019. 122 с.
13. Тенденции технологии IoT в 2023 году. URL: https://habr.com/ru/companies/timeweb/articles/691610.
14. Что такое интернет вещей и как он устроен. URL: https://trends.rbc.ru/trends/industry/5db96f769a7947561444f118.
15. Шиков С.А. Проблемы информационной безопасности: интернет вещей // Вестник Мордовского университета. 2017. Т. 27. № 1. С. 27-40.
16. Шумбасов А.М., Свешников И.А. Блокчейн и криптовалюта интернет вещей // Молодежь. Общество. Современная наука, техника и инновации. 2022. № 21. С. 190-191.
17. ISO/IEC 27001 Системы менеджмента информационной безопасности. URL: https://www.iso.org/ru/standard/27001.
18. Nozari H., Fallah M., Kazemipoor H., Najafi S.E. Big data analysis of iot-based supply chain management considering fmcg industries // Biznes-Informatika. 2021. Vol. 15. No 1. P. 78-96.

The development of the Internet of Things and the problems of ensuring its security

Viktor L. Akap'ev

PhD in Pedagogy,
Associate Professor of the Department of Information and Computer Technologies in the Activities of the Department of Internal Affairs,
Belgorod Law Institute of the Ministry of Internal Affairs of Russia named after I.D. Putilin,
308024, 71 Gor'kogo str., Belgorod, Russian Federation;
e-mail: nazhukova2008@yandex.ru

Sergei E. Savotchenko

Doctor of Physical and Mathematical Sciences, Associate Professor,
Professor of the Department of Mathematics,
Russian State Geological Exploration University named after Sergo Ordzhonikidze,
117485, 23 Miklukho-Maklaya str., Moscow, Russian Federation;
e-mail: nazhukova2008@yandex.ru

Natal'ya A. Zhukova

PhD in Law, Associate Professor,
Head of the Department of Forensic Examination and Criminology,
Belgorod State National Research University,
308015, 85 Pobedy str., Belgorod, Russian Federation;
e-mail: nazhukova2008@yandex.ru

Abstract

The large-scale introduction of the Internet of Things requires the legislator to improve the legal provision of personal information security and a global rethinking by lawyers of the process of formation of the information society. The object of the study is the vulnerabilities of the Internet of Things in the context of ensuring the information security of professional activity against the background of the widespread and dynamically developing use of computer equipment, information technologies and means of communication, the intersection with the IoT space of the critical information infrastructure of the Russian Federation.

For citation

Akap'ev V.L., Savotchenko S.E., Zhukova N.A. (2024) Razvitie Interneta veshchei i problemy obespecheniya ego bezopasnosti [The development of the Internet of Things and the problems of ensuring its security]. *Voprosy rossiiskogo i mezhdunarodnogo prava* [Matters of Russian and International Law], 14 (2A), pp. 257-267. DOI: 10.34670/AR.2024.95.70.051

Keywords

Basic principles of IoT, information security, Internet of things, information system, cybersecurity, operational technologies, IoT technologies, requirements for IoT systems, IoT vulnerabilities.

References

1. *Aktual'nost' problemy obespecheniya bezopasnosti informatsii* [The relevance of the problem of ensuring information security]. Available at: https://searchinform.ru/informatsionnaya-bezopasnost/osnovy-ib/osnovnye-aspekty-informatsionnoj-bezopasnosti/osnovnye-printsipy-obespecheniya-informatsionnoj-bezopasnosti/problemy-obespecheniya-bezopasnosti-informatsii [Accessed 12/03/2024].
2. *Chto takoe internet veshchei i kak on ustroen* [What is the Internet of Things and how does it work]. Available at: https://trends.rbc.ru/trends/industry/5db96f769a7947561444f118 [Accessed 14/03/2024].
3. *Ezda po vole khakera* [Driving at the behest of a hacker]. Available at: https://www.kommersant.ru/doc/2773532 [Accessed 12/03/2024].
4. *Informatsionnaya bezopasnost' avtomatizirovannykh sistem: ponyatie, metody obespecheniya* [Information security of automated systems: concept, methods of provision]. Available at: https://gb.ru/blog/informatsionnaya-bezopasnost-avtomatizirovannykh-sistem [Accessed 16/03/2024].
5. *Internet veshchei* [Internet of things]. Available at: https://sber.pro/digital/education/internet_vesshei [Accessed 12/03/2024].
6. *ISO/IEC 27001 Sistemy menedzhmenta informatsionnoi bezopasnosti* [ISO/IEC 27001 Information security management systems]. Available at: https://www.iso.org/ru/standard/27001 [Accessed 12/03/2024].
7. *Kazino vzlomali cherez termostat v akvariume* [The casino was hacked through the thermostat in the aquarium]. Available at: https://habr.com/ru/companies/globalsign/articles/354256 [Accessed 12/03/2024].
8. *Kommunikatsionnye tekhnologii interneta veshchei. Chto eto takoe* [Communication technologies of the Internet of things. What it is]. Available at: https://tulasprav.ru/articles/kommunikatsionnye-tehnologii-interneta-veschey-chto-eto-takoe.html [Accessed 23/03/2024].
9. Nozari H., Fallah M., Kazemipoor H., Najafi S.E. (2021) Big data analysis of IOT-based supply chain management considering FMCG industries. *Biznes-Informatika* [Business-Informatics], 15 (1), pp. 78-96.
10. Pikover A.V. (2021) Internet veshchei i promyshlennyi internet veshchei v KNR [Internet of Things and Industrial Internet of Things in the People's Republic of China]. *Sbornik statei ezhegodnoi nauchnoi konferentsii Tsentra ekonomicheskikh i sotsial'nykh issledovanii Kitaya Instituta Dal'nego Vostoka RAN «Sotsial'no-ekonomicheskie itogi 13-i pyatiletki KNR (2016-2020 gg.) i zadachi 14-i pyatiletki (2021-2025 gg.)»* [Proc. Conf. "Sotsial'no-ekonomicheskie itogi 13-i pyatiletki KNR (2016-2020) i zadachi 14-i pyatiletki (2021 -2025 gg.)"]. Moscow, pp. 195-209.
11. *Portal iot.ru «Novosti Interneta veshchei»* [Portal iot.ru "Internet of Things News"]. Available at: https://iot.ru [Accessed 12/03/2024].
12. Rogacheva N.V. (2021) Internet veshchei: obzor osnovnykh problem i zadach [Internet of Things: overview of the main problems and challenges]. *Languages in professional communication* [Languages in professional communication], pp.

558-563.
13. Shikov S.A. (2017) Problemy informatsionnoi bezopasnosti: internet veshchei [Problems of information security: Internet of things]. *Vestnik Mordovskogo universiteta* [Bulletin of Mordovian University], 27 (1), pp. 27-40.
14. Shumbasov A.M., Sveshnikov I.A. (2022) Blokchein i kriptovalyuta internet veshchei [Blockchain and cryptocurrency Internet of things]. *Molodezh'. Obshchestvo. Sovremennaya nauka, tekhnika i innovatsii* [Youth. Society. Modern science, technology and innovation], 21, pp. 190-191.
15. Suomalainen A. (2019) *Internet veshchei: video, audio, kommutatsiya* [Internet of things: video, audio, switching]. Moscow: DMK Press Publ.
16. *Tendentsii tekhnologii IoT v 2023 godu* [IoT technology trends in 2023]. Available at: https://habr.com/ru/companies/timeweb/articles/691610 [Accessed 12/03/2024].
17. Vereshchagina E.A., Kapetskii I.O., Yarmonov A.S. (2021) *Problemy bezopasnosti Interneta veshchei* [Internet of Things security issues]. Moscow: Mir nauki,. Available at: https://izd-mn.com/PDF/20MNNPU21.pdf [Accessed 12/03/2024].
18. *Virus VPNFilter: opisanie, vozmozhnosti, spisok uyazvimykh ustroistv* [VPNFilter virus: description, capabilities, list of vulnerable devices]. Available at: https://networkguru.ru/virus-vpnfilter-opisanie-vozmozhnosti-ustroystva [Accessed 22/03/2024].