УДК 004 **Информационные технологии**

Сексембаева Манара Ануаровна, *магистр естественных наук, преподаватель, Евразийский национальный университет им. Л. Н. Гумилева*

ОСОБЕННОСТИ ОБЕСПЕЧЕНИЯ БЕЗОПАСНОСТИ В ПРОМЫШЛЕННОМ ИНТЕРНЕТЕ ВЕЩЕЙ

Аннотация: Мир интернет вещей (Internet of Things, IoT) проникает во все новые области жизни человека. В ближайшее время отдельные IoT-решения будут обгонять стандартизацию и унификацию, что будет ограничивать их совместимость и повышать риски безопасности. В данной статье мы проанализируем особенности безопасности промышленного интернета вещей и дадим обзор актуальных угроз, опираясь на последние стандарты, публикации и рекомендации.

Ключевые слова: интернет вещей; промышленный интернет вещей, угрозы безопасности в IIoT; атака, защита.

Abstract: The world of the Internet of Things (Internet of Things, IoT) is penetrating into all new areas of human life. In the near future, individual IoT solutions will outrun standardization and unification, which will limit their compatibility and increase security risks. In this article we will analyze the security features of the industrial Internet of things and give an overview of current threats, based on the latest standards, publications and recommendations.

Keywords: internet of things; industrial internet of things, security threats in IIoT; attack, defense.

Интернет вещей (Internet of Things, IoT) – это совокупность различных вещей, объединённых между собой произвольными каналами связи и

произвольными протоколами, но использующих единый протокол (IP) для доступа к единой глобальной сети (Интернет).

Вещь – применительно к интернету вещей означает предмет физического мира (физические вещи) или информационного мира (виртуальные вещи), который может быть идентифицирован и интегрирован в сети связи [4]. В Рекомендации МСЭ Y.2060 также отдельно выделено понятие *устройство* – применительно к интернету вещей означает элемент оборудования, который обладает обязательными возможностями связи и дополнительными возможностями измерения, срабатывания, а также ввода, хранения и обработки данных [4].

Промышленный интернет вещей (Industrial Internet of Things, IIoT) - интернет вещей для корпоративного / отраслевого применения.

Заметим, что доступ к глобальной сети необязателен. Например, «умный дом», состоящий из набора вещей, обменивающихся с помощью Wi-Fi или Bluetooth с центральным контроллером, может и не выходить в Интернет. Аналогично, корпоративная сеть «умных вещей» может запретить им непосредственно реализовывать удалённый доступ или существенно его ограничить.

Учитывая разнородность приложений по конечному пользователю (частное лицо, предприятие, государство), система стандартов будет многоуровневой, различной по степени охвата и детализации.

К данному моменту (май 2019 г.) разработаны следующие документы, которые носят обобщающий и рекомендательный характер:

- Рекомендация Y.2060 Международного союза электросвязи при ООН [4];
- Всемирный форум IoT(IoT World Forum), семиуровневая модель IoT [2];
- Good Practices for Security of Internet of Things in the context of Smart Manufacturing, The European Union Agency for Network and Information Security [3].

В конце 2019 года был опубликован стандарт ISO/TR 22100-4:2018 «Безопасность производственного оборудования — Связь с ISO 12100 — Часть 4: Руководство для производителей оборудования по рассмотрению соответствующих аспектов информационной безопасности (кибербезопасности)» [9], целью которого является «усиление безопасности промышленного IoT оборудования».

Промышленный интернет вещей – фундамент четвёртой промышленной революции. 46-й Международный экономический форум 2016 года в Давосе прошёл под лозунгом «Четвёртой промышленной революции», определив его характерные особенности: слияние технологий и размытие граней между физическими, цифровыми и биологическими сферами.

Впервые концепция четвёртой промышленной революции, или «Индустрии 4.0», была сформулирована в Германии на Ганноверской выставке в 2011 году, в связи с начавшимся массовым внедрением «киберфизических систем» в заводские процессы [11, с.24]. Продвигаясь в этом направлении, США в 2014 году создают некоммерческий консорциум Industrial Internet, среди учредителей которого General Electric, AT&T, IBM и Intel. Германия ежегодно инвестирует по 40 миллиардов евро в новую интернет-инфраструктуру и создание глобальных стандартов [10]. Аналогичные программы разрабатываются и внедряются в Китае, Южной Корее и Японии.

Эксперты ENISA определяют «Индустрию 4.0» как «смену парадигмы в пользу цифровых, интегрированных и интеллектуальных цепочек создания стоимости для обеспечения распределенного принятия решений на производстве с внедрением новых киберфизических технологий, таких как IoT» [8, с.12].

Промышленный интернет вещей интегрирует производство с ИТ, данные пользователей с машинными данными и позволяет машинам общаться друг с другом (рис.1). В результате управление вещами, устройствами и машинами становится автономным, гибким, эффективным и ресурсосберегающим.

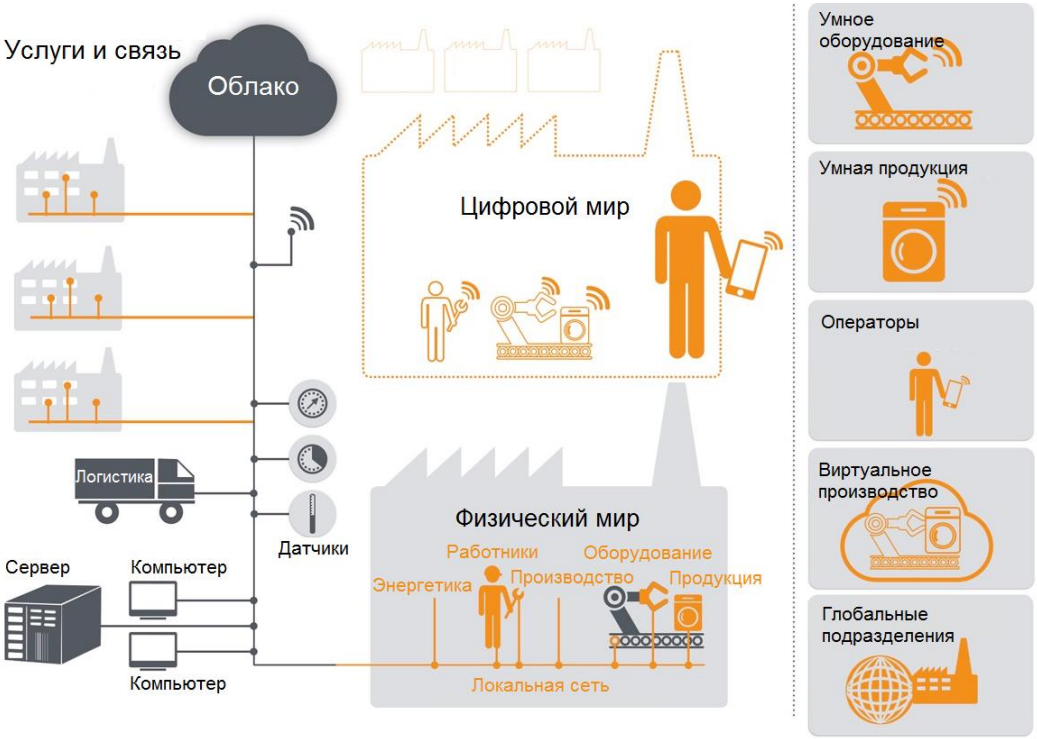

Рис.1. Концепция «Индустрия 4.0». (http://www.industries-4.com/category/industrie-4-0).

Традиционная модель взаимодействия «поставщик – потребитель» в новой концепции кардинально меняется благодаря следующим факторам:

- автоматизации процесса мониторинга и управления жизненным циклом оборудования;
- организации эффективных самооптимизирующихся цепочек от предприятий – поставщиков до компаний – конечных потребителей;
- переходу к моделям «экономики совместного использования», когда оборудование оплачивается заказчиком по факту использования его функций и т.п.

Таким образом, промышленный интернет вещей приводит к организационно-технологической трансформации производства, позволяющей интегрировать материальные, транспортные, человеческие, инженерные и иные ресурсы в практически неограниченно масштабируемые программно-управляемые виртуальные пулы (shared economy) и предоставлять пользователю не сами устройства, а результаты их использования (функции устройств) за счет реализации сквозных (cross-functional) производственных и бизнес-процессов.

Угрозы безопасности в сфере промышленного интернета вещей. Эксперты признают, что в настоящее время безопасность промышленного интернета вещей обеспечена слабо, поскольку беспроводной трафик часто не шифруется, не предусмотрены пароли достаточной сложности, используются уязвимые протоколы и программное обеспечение, а также повсеместно наблюдается несовместимость, отсутствие стандартов и многие другие факторы.

В декабре 2017 года компания FireEye опубликовала данные об атаке, которая вызвала сбой в работе системы противоаварийной защиты предприятия. Атака не привела к серьезным последствиям, но данный инцидент показал возможность нанести физический ущерб и прервать выполнение критически важных технологических процессов. Злоумышленниками было специально создано вредоносное ПО Triton для вмешательства в работу систем противоаварийной защиты Triconex Safety Instrumented System (SIS) от Schneider Electric [1].

6 апреля 2018 года по всему миру были зафиксированы массовые атаки на коммутаторы Cisco IOS. Атаки привели к сбою в работе некоторых интернет-провайдеров, дата-центров и веб-сайтов. Злоумышленники использовали уязвимость CVE-2018-0171 в программном обеспечении Cisco Smart Install Client [7]. По результатам исследований команды Cisco Talos, в мире насчитывается более 168 000 потенциально подверженных ей устройств. Кроме того, среди компаний, подвергшихся атакам, оказались и объекты критической инфраструктуры.

В апреле 2018 года был обнаружен ботнет, состоящий из интернет-телевизоров. Этот ботнет использовался для осуществления DDoS-атак на организации финансового сектора [12].

В мае 2018 года было обнаружено новое вредоносное ПО VPNFilter, которое заразило не менее 500 тысяч маршрутизаторов и устройств хранения данных (NAS) в 54 странах мира [13].

В июне 2018 года стало известно о масштабной кибератаке с территории Китая на телекоммуникационные предприятия, операторов спутников связи, а также оборонных подрядчиков в США и странах Юго-Восточной Азии. Для заражения вредоносным ПО злоумышленники использовали обычные инструменты и средства администрирования PsExec, Mimikatz, WinSCP и LogMeIn [14].

В июле 2018 года появилось сообщение о кибератаке на медицинское учреждение в Тюмени. Эта атака показала, что злоумышленники могут не только выводить из строя компьютерные системы, но и оказывать непосредственное влияние на процесс лечения пациентов [5].

Заметим, что пока пишутся эти строки, по всей планете не прекращаются атаки с помощью фишинговых писем, которые замаскированы под обычные коммерческие предложения, а по содержанию соответствуют деятельности атакуемой организации и учитывают специфику работы сотрудника — получателя письма. Основной целью атакующих является кража денежных средств со счетов предприятия. Очевидно, что, помимо финансовых потерь, данные атаки приводят к утечке конфиденциальных данных организации.

По данным лаборатории Касперского количество атакованных автоматизированных систем управления в первом полугодии 2018 года выросло до 41,2% (рис.2).

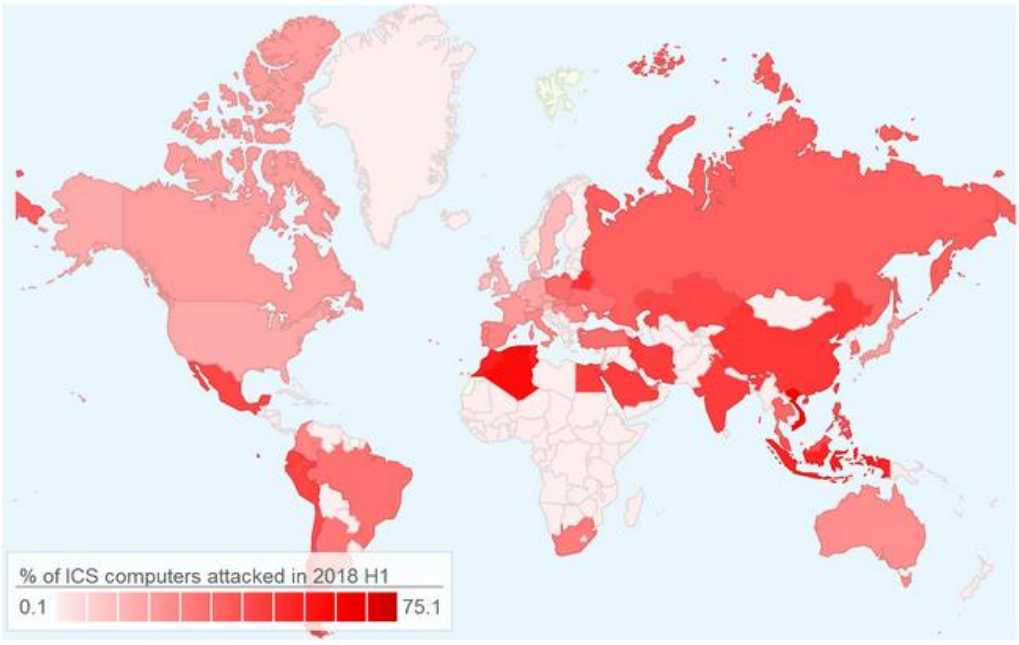

Рис.2. География атак на системы промышленной автоматизации, первое полугодие 2018 [2].

За 2018 наибольшее количество уязвимостей было выявлено в:

- инженерном ПО (143),
- SCADA/HMI-компонентах (81),
- сетевых устройствах промышленного назначения (66),
- ПЛК (программируемых контроллерах) (47).

Рис.3. Распределение уязвимостей по компонентам АСУ в 2018 году [14].

Взаимосвязанность вещей и устройств в IIoT, сама сущность новой парадигмы «Индустрии 4.0» предоставляет возможность не только для цифровых, но и для физических атак (рис.4).

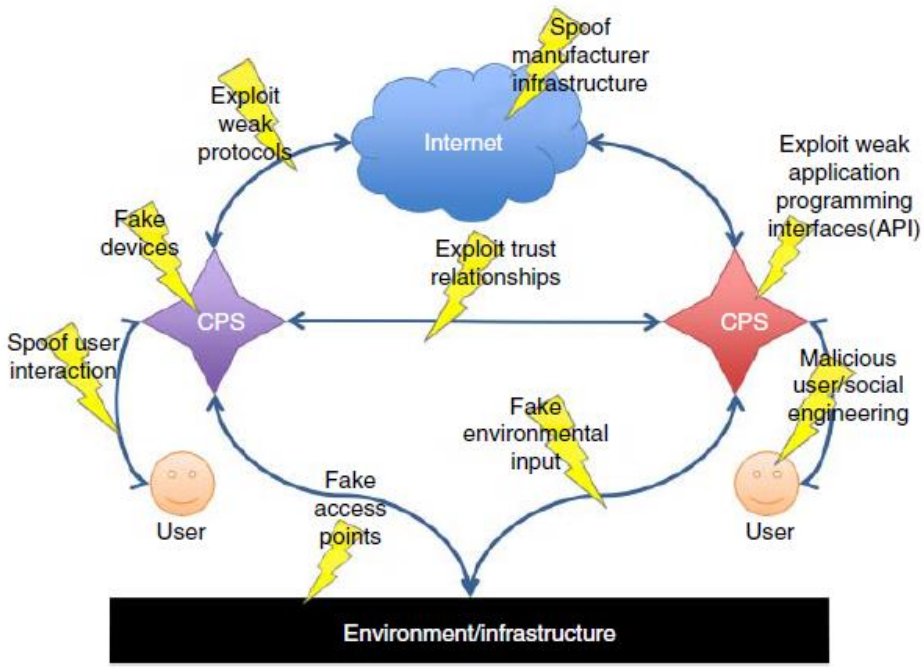

Рис.4. Основные уязвимости киберфизических систем [11, с.7].

Уязвимости цифрового и физического мира не просто суммируются, они умножаются [11, с. 6].

На сегодня, к списку слабых мест и процессов, через которые киберфизическая система может быть атакована и повреждена, следует отнести:

- продолжающийся переход на IPv6;
- системы питания датчиков;
- стандартные учётные записи от производителя, слабая аутентификация;
- отсутствие поддержки со стороны производителя для устранения уязвимостей;
- трудности обновления ПО и ОС;
- использование текстовых протоколов и ненужных открытых портов;
- использование незащищённых мобильных технологий;
- использование незащищённой облачной инфраструктуры;
- использование уязвимого ПО;
- человеческий фактор.

Подробный перечень угроз, характерных для IIoT, мы находим в разделе 3.1 документа ENISA [8] (табл.1).

Согласно лучшим практикам ENISA	**Переводной термин**	**Описание**
Nefarious activity / Abuse	Недобросовестная деятельность и злоупотребления	Различные манипуляции с данными и оборудованием
Eavesdropping / Interception / Hijacking	Прослушивание / перехват / взлом	Сбор информации и взлом системы
Unintentional damages (accidental)	Непреднамеренные (случайные) повреждения	Ошибки в конфигурировании, администрировании и использовании
Outages	Отключения	Простои в работе, связанные с отключением электропитания, коммуникаций или сервисов
Disaster	Катастрофы	Разрушительные внешние воздействия природного и техногенного характера
Physical attack	Физические атаки	Вандализм и саботаж, вывод из строя устройств и оборудования
Failures / Malfunctions	Отказы и ошибки в работе	Случайные отказы устройств и оборудования, отказы у провайдеров услуг, ошибки в разработке ПО, наличие уязвимостей
Legal	Нарушения законодательства	Нарушение требований законов и контрактов

Таблица 1. Угрозы безопасности в IIoT согласно ENISA.

Свою точку зрения на базовую систему безопасности представила компания Cisco Systems в дополнение к эталонной модели Всемирного форума IoT [6] На рис.5 показан соответствующий фреймворк, связанный с логической структурой IoT.

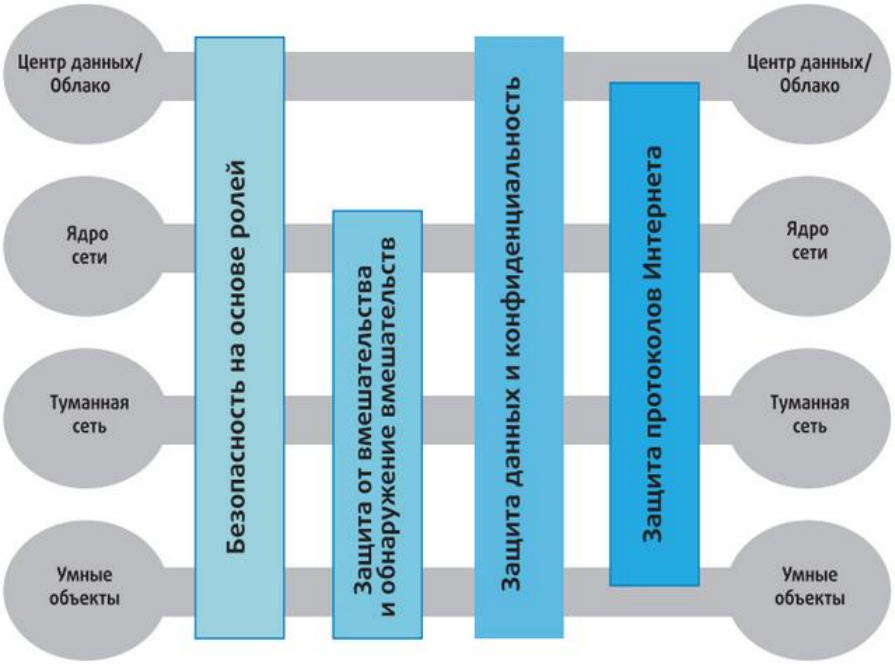

Рис.5. Базовая среда безопасности IoT, связанная с логической структурой (Cisco Systems)[6].

Специалисты Cisco выделяют четыре уровня поддержки безопасности:

- Безопасность на основе ролей (Role-Based Access Control, RBAC), согласно которой назначаются права доступа по профилям, основанным на ряде метрик, а не отдельным пользователям. Пользователям, в свою очередь, сопоставляются различные профили, либо статически, либо динамически, соответственно обязанностям.
- Защита от вмешательства и обнаружение вмешательств: эта функция критична на уровне устройств и туманной сети, но распространяется также и на уровень ядра сети. Все эти уровни могут использовать компоненты, физически находящиеся вне физически охраняемой территории предприятия.
- Защита данных и конфиденциальность: эти функции охватывают все уровни архитектуры.
- Защита протоколов Интернета: защита данных от подслушивания и перехвата на всех уровнях.

С точки зрения специалистов ENISA, лучшие практики, направленные на защиту компонентов IIoT от угроз следует разделить на три основных класса:

политики безопасности, организационные мероприятия, технические мероприятия (рис.6).

Рис.6. Структура лучших практик ENISA, направленных на защиту компонентов IIoT от угроз [8, с. 36].

Данный перечень практик детализуется в документе ENISA в виде таблиц, где сделана привязка к группам угроз и даны ссылки на документы, поддерживающие применение той или иной практики [8, Приложение B].

Несмотря на то, что рынок промышленного интернета вещей оценивается в сотни миллиардов долларов, мы оказались не готовы к жёстким требованиям, которые он предъявляет в области безопасности.

Сегодня на уровне регуляторов первоочередной задачей является разработка единых стандартов, терминологии и классификации, привлечение ведущих специалистов и обобщение лучших практик.

На уровне предприятий, производителей оборудования и ПО необходимо разрабатывать и внедрять эффективные политики безопасности, поддерживать актуальные знания сотрудников в этой области, развивать системы тестирования и аудита.

Промышленный интернет вещей постепенно преобразовывает наш мир. Чтобы изменения были позитивными, всегда необходимо помнить о приоритете – комплексной безопасности экосистемы IIoT.

Библиографический список:

1. Атака TRITON. Комментарий эксперта Kaspersky Lab ICS CERT // - [электронны ресурс] – режим доступа – URL: https://ics-cert.kaspersky.ru/news/2017/12/18/triton/ (дата обращения 10.05.2019).

2. Ландшафт угроз для систем промышленной автоматизации: первое полугодие 2018 // - [электронны ресурс] – режим доступа – URL: https://ics-cert.kaspersky.ru/reports/2018/09/06/threat-landscape-for-industrial-automation-systems-h1-2018/#_Toc523499583 (дата обращения 10.05.2019).

3. Ландшафт угроз для систем промышленной автоматизации. Второе полугодие 2018 // - [электронны ресурс] – режим доступа – URL: https://ics-cert.kaspersky.ru/reports/2019/03/27/threat-landscape-for-industrial-automation-systems-h2-2018/ (дата обращения 10.05.2019).

4. Обзор интернета вещей. Рекомендация МСЭ-Т Y.2060 // Сектор стандартизации электросвязи МСЭ, 06/2012 - 22 с. // - [электронны ресурс] – режим доступа – URL: https://www.itu.int/rec/T-REC-Y.2060-201206-I (дата обращения 10.05.2019).

5. Тюменский центр нейрохирургии подвергся кибератаке во время операции на головном мозге ребенка // - [электронны ресурс] – режим доступа – URL: https://72.ru/text/incident/65119911/ (дата обращения 10.05.2019).

6. CISCO, «The Internet of Things Reference Model», White Paper, June 2014 - [электронны ресурс] – режим доступа – URL: http://cdn.iotwf.com/resources/71/IoT_Reference_Model_White_Paper_June_4_2014.pdf (дата обращения 10.05.2019).

7. Cisco IOS and IOS XE Software Smart Install Remote Code Execution Vulnerability - [электронны ресурс] – режим доступа – URL:

https://tools.cisco.com/security/center/content/CiscoSecurityAdvisory/cisco-sa-20180328-smi2 (дата обращения 10.05.2019).

8. Good Practices for Security of Internet of Things in the context of Smart Manufacturing, The European Union Agency for Network and Information Security. November 19, 2018 - [электронны ресурс] – режим доступа – URL: www.enisa.europa.eu (дата обращения 10.05.2019).

9. ISO/TR 22100-4:2018. Safety of machinery — Relationship with ISO 12100 — Part 4: Guidance to machinery manufacturers for consideration of related IT-security (cyber security) aspects // https://www.iso.org/obp/ui/#iso:std:iso:tr:22100:-4:ed-1:v1:en.

10 IT Security in Industrie 4.0 Action fields for operators. - Federal Ministry for Economic Affairs and Energy (BMWi), Berlin, November 2016 - [электронны ресурс] – режим доступа – URL: https://www.plattform-i40.de/PI40/Redaktion/EN/Downloads/Publikation/guideline-it-security-i40-action-fields.pdf?__blob=publicationFile&v=3 (дата обращения 10.05.2019).

11. Houbing Song (ed.). Security and Privacy in Cyber-Physical Systems. - John Wiley & Sons, 2018. - 457 p.

12. Mirai-Variant IoT Botnet Used to Target Financial Sector in January 2018 // - [электронны ресурс] – режим доступа – URL: https://www.recordedfuture.com/mirai-botnet-iot/ (дата обращения 10.05.2019).

13. New VPNFilter malware targets at least 500K networking devices worldwide // - [электронны ресурс] – режим доступа – URL: https://blog.talosintelligence.com/2018/05/VPNFilter.html (дата обращения 10.05.2019).

14. Thrip: Espionage Group Hits Satellite, Telecoms, and Defense Companies // [электронны ресурс] – режим доступа – URL: https://www.symantec.com/blogs/threat-intelligence/thrip-hits-satellite-telecoms-defense-targets (дата обращения 10.05.2019).