Современные исследовательские проекты ЕС и онтологии цифровой безопасности Европы

И.А.Соколов, В.П.Куприяновский, Д.Е.Намиот, В.А.Сухомлин, О.Н.Покусаев, А.И.Лавров, Ю.И.Волокитин

***Аннотация*— В статье рассматриваются вопросы, связанные с кибер-безопасностью в цифровой экономике. Работа представляет собой обзор исследовательских проектов, финансируемых Европейским сообществом, которые затрагивают различные вопросы кибер-безопасности. Авторам статьи представляется, что российским исследователям в данной области будет полезно ознакомиться с практикой ЕС в данном направлении. Большое внимание в статье уделено работам по созданию практических онтологий. Их результаты публикуются для широкого обсуждения и практического использования. Разработанные формальные онтологии на искусственных языках могут быть стыкованы между собой и призваны обеспечить совместимость данных и приложений, а также их прозрачность на протяжении жизненных циклов. Именно онтологический подход позволяет рассчитывать основные контрольные показатели проектов и, например, гарантировать выполнение заявленных бизнес-правил.**

***Ключевые слова*—кибер-безопасность, онтологии, H2020.**

I. Введение

Подписанные Президентом России решения о переходе к цифровой экономике [1,2,3] содержат сбалансированный подход к ее развитию в России, во взаимодействии со странами, входящими в ЕАЭС. Решение [2] относится к развитию информационного общества, а указ [3] к экономической безопасности. В работах [4-12] были представлены различные реализующиеся проекты цифровой экономики и было показано, что они затрагивают практически все сферы деятельности человека в новом экономическом укладе.

В статье [5] авторы привели обширную таблицу угроз новым технологиям и попытались проиллюстрировать реализацию цифровой безопасности в стандартах на самую сложную сегодня инфраструктуру – умные города. Эта публикация вызвала значительный интерес читателей. Чтобы ответить на их вопросы и предложить для исследователей некоторые направления, мы решили подготовить эту статью.

Так как страны Европы и, например, ЕС имеют свои политики и стратегии экономического развития [4] и, соответственно, реализации [7-11] мы для этой статьи выбрали то, что авторам представляется полезным российским исследователям и практикам – практику ЕС. Как было показано в работе [7] и ряде других, практическая онтология стала одним из основных средств реализации крупных систем и, в том числе, цифровой безопасности.

Как правило, это то, что называют программным обеспечением для управления онтологиями на всех этапах их жизненного цикла. Обычно это:

- Редакторы Онтологий (средство создания, хранения и редактирования онтологий). Например, Protege, OSA.Ontology.Editor
- Средства Онто.Колаборации (коллективная разработка онтологий: аннотирование, согласования и утверждения онтологий) Например, OWL, OSA.Colaboration
- Средства Взаимодействия Онтологий (интеграция, объединение, федерирование и пр. более 30 операций между онтологиями). Например: OWL, Protege, OSA.Ontology.Editor
- Средства Верификации и Валидации Онтологий, Резонеры (инструменты анализа логической непротиворечивости и правил вывода). Зачастую, они встроены непосредственно в Редакторы Онтологий
- Средства Визуализации Онтологий (разнообразные аналитические представления онтологий). Например: OSA.Cube
- Точки доступа знаниям в онтологиях (SPARQL, OSA.Cube)
- Языки ограничений и аксиоматики (типа SHACL, OSA.Express).

Работа по созданию практических онтологий всегда предусматривает тщательные научно-практические исследования, которые сегодня осуществляются в виртуальных кабинетах, комнатах и площадках. Их результаты публикуются для широкого обсуждения и практического использования. Разработанные формальные онтологии на искусственных языках могут

Статья получена 20 февраля 2018.
И.А.Соколов - Национальный центр компетенций в цифровой экономике МГУ, ФИЦ «Информатика и управление» РАН (email: isokolov@ipiran.ru)
В.П.Куприяновский - Национальный центр компетенций в области цифровой экономики (email: vpkupriyanovsky@gmail.com)
Д.Е.Намиот - МГУ имени М.В. Ломоносова (e-mail: dnamiot@gmail.com)
В.А.Сухомлин - МГУ имени М.В. Ломоносова (e-mail: sukhomlin@mail.ru)
О.Н.Покусаев - Центр цифровых высокоскоростных транспортных систем РУТ (МИИТ) (email: o.pokusaev@rut.digital)
А.И.Лавров - ИТЦ Союз (email:lavrov63@gmail.com)
Ю.И.Волокитин - ООО ТАС (email: i18021958@gmail.com)

быть стыкованы между собой и призваны обеспечить совместимость данных и приложений или прозрачность на протяжении жизненных циклов. Именно онтологический подход позволяет рассчитывать KPI и, например, гарантировать необходимую латентность в работе информационных систем и идентификацию объектов и субъектов, участвующих в бизнес-процедурах.

Авторы включили в эту статью описание некоторых исследовательских проектов в области цифровой безопасности, разбив их на небольшие разделы. В предположении, что читатель захочет посмотреть более детально эти материалы, мы снабдили сами проекты их символикой и веб адресами. Однако для одного из проектов (RECRED) мы подобрали те завершенные работы, которые доступны для анализа российскими специалистами.

II. Контроль доступа

RECRED - это европейский проект (программа H2020), целью которого является разработка и внедрение механизмов, которые привязывают все требования к контролю доступа (AC) к мобильным устройствам, которые пользователи обычно используют и переносят. Он направлен на создание интегрированного решения контроля доступа (AC) следующего поколения, которое: i) решает следующие проблемы, связанные с недостатками существующих методов аутентификации, ii) согласовывается с современными технологическими тенденциями и возможностями, iii) предлагает унифицированный контроль доступа которая подходит для множества вариантов использования, которые включают онлайн-аутентификацию и авторизацию через встроенное мобильное устройство, и iv) является достижимой и выполнимой для реализации в существующих продуктах в рамках и сроках проекта. Website: https://www.recred.eu/

Как мы и обещали читателю во введении, для этого проекта сделана подборка опубликованных результатов исследований [13-29]. Объем этих отработанных и согласованных документов существенно превышает 1000 страниц, и они согласованны с представителями крупных заинтересованных компаний (смотри веб и списки участников в [13-29]). В этот объем естественно не включаются публикации в научных изданиях, которые, хоть и являются частью проделанной работы, но учитываются на сайте отдельно.

AMBER («Enhanced Mobile BiomEtRics») - инновационная обучающая сеть Marie Skłodowska-Curie, посвященная целому ряду текущих проблем, стоящих перед биометрическими решениями на мобильных устройствах. AMBER будет включать в себя десять интегрированных проектов раннего этапа исследований по программе Марии Склодовска-Кюри (ESR) в пяти университетах ЕС. Сеть оказывает непосредственную поддержку семи промышленным партнерам. Целью Сети является сопоставление экспертного и промышленного опыта в масштабах всей Европы, подготовка и оснащение следующего поколения исследователей для определения, исследования и внедрения решений, а также разработки решений и теории для обеспечения безопасной, вездесущей и эффективной аутентификации, защищая конфиденциальность граждан. Website: https://www.amber-biometrics.eu/

Целью проекта **OPERANDO** является определение, внедрение, тестирование на местах, проверка и использование инновационной платформы обеспечения соблюдения конфиденциальности, которая позволит использовать бизнес-парадигму конфиденциальности как услуги (PaaS) и рынок онлайн-сервисов конфиденциальности. Проект OPERANDO будет интегрировать и расширять современное состояние для создания платформы, которая будет использоваться независимыми поставщиками услуг конфиденциальности (PSP) для обеспечения всестороннего соблюдения конфиденциальности пользователя в виде специализированной онлайн-службы под названием «Privacy Authority». Платформа OPERANDO будет поддерживать гибкие и жизнеспособные бизнес-модели, включая ориентацию на отдельные сегменты рынка, такие как государственное администрирование, социальные сети и Интернет. Website: https://www.operando.eu

Отсутствие прозрачности в отношении методов отслеживания в системе онлайн-рекламы и типов информационных компаний, собирающих информацию о пользователях, создает все большую озабоченность в обществе. **TYPES** - это европейский проект (программа H2020), цель которого - справиться с этой задачей, определяя, внедряя и подтверждая статус до рынка, целостную структуру технологий и инструментов, гарантирующих прозрачность и конфиденциальность, дает конечный пользовательский контроль над количеством информации, которое он / она желает поделиться, и определяет решения по обеспечению конфиденциальности. В частности, эти инструменты должны позволить конечному пользователю: i) настроить параметры конфиденциальности, чтобы только информация, разрешенная конечным пользователем, собиралась платформами онлайн-рекламы; ii) понимать поток своей информации в экосистеме онлайн-рекламы и то, как она используется; iii) выявлять эпизоды сбора информации, происходящие без согласия и идентифицировать правонарушителя; iv) знать ценность своих данных. TYPES продемонстрирует решения, которые защищают конфиденциальность пользователя, а также позволят им контролировать, как их данные используются поставщиками услуг для рекламы. В то же время TYPES упростит проверку соблюдения прав пользователей в Интернете и обмен личными данными для разумной добавленной стоимости для пользователей. Website: http://www.types-project.eu/

Проект «Флаг конфиденциальности» - это европейский исследовательский проект по защите персональных данных. Его эксперты в области права и ИКТ разработали инновационную методологию - Универсальную методологию оценки области риска конфиденциальности (**UPRAAM**) - для оценки соответствия приложений, веб-сайтов и развертывания Интернета Вещей в соответствии с Общим регламентом защиты данных Европейского Союза (GDPR) и Швейцарским Закон о защите данных. Используя UPRAAM, Privacy Flag разрабатывает набор инструментов, позволяющих гражданам проверять, соблюдаются ли их права как субъектов данных, а также инструменты и услуги, которые помогают компаниям соблюдать требования к защите персональных данных. Флаг конфиденциальности совместно финансируется Европейской комиссией и Государственным секретариатом Швейцарии по вопросам образования, исследований и инноваций. Website: http://privacyflag.eu/

ARIES создаст всеобъемлющую структуру технологий, процессов и функций безопасности для управления физической и виртуальной идентификацией, что позволит в дальнейшем создать европейскую экосистему электронного идентификатора, заслуживающую доверия для граждан, которая поддерживает возможности управления полномочиями правоохранительных органов и устраняет новые угрозы в кибер-безопасности. ARIES предлагает новые способы повышения безопасности электронного документооборота и управления идентификационными документами в соответствии с целями безопасности Союза / ЕС в области безопасности, связанными с установлением четких правил, обеспечивающих полное соблюдение принципов защиты данных. В то время как правоохранительные органы получают доступ к данным, он должен защищать неприкосновенность частной жизни граждан от кибер-преступности и кражи личных данных. Website: http://aries-project.eu/

CREDENTIAL - это исследовательский проект, финансируемый ЕС, который разрабатывает, тестирует и демонстрирует инновационные облачные сервисы для хранения, управления и обмена информацией о цифровой идентификации и других высоко-критических персональных данных с явно более высоким уровнем безопасности, чем другие текущие решения. Основная идея и амбиция CREDENTIAL - обеспечить сквозную безопасность и улучшить конфиденциальность в службах управления облачной идентификацией для управления безопасным доступом. Это достигается за счет развития новых криптографических технологий и улучшения сильных механизмов аутентификации. Website: https://credential.eu/

III. Доверенные eServices

Основной задачей проекта **FutureTrust** является поддержка практической реализации регламента eIDAS (2014/910 / EU) по электронной идентификации (eID) и доверенных услуг для электронных транзакций на внутреннем рынке и облегчение использования и распространения надежных eID и технологии электронной подписи в Европе и за ее пределами, с тем чтобы обеспечить юридически значимые электронные транзакции по всему миру. С этой целью проект FutureTrust будет основываться на результатах, разработанных в рамках предыдущих исследовательских и масштабных пилотных проектов, и призван интегрировать существующие доверительные службы, которые в основном связаны с квалифицированными сертификатами, электронными подписями и штампами времени, с будущей концепцией функциональной совместимости eID и проведением исследований, проектирования инновационные решения и обеспечить реализацию Open Source для недавно введенных трастовых служб, связанных с проверкой, сохранением и мобильным созданием квалифицированных электронных подписей и печатей. Website: https://www.futuretrust.eu/

Цель **LIGHTest** - создать глобальную инфраструктуру междоменного доверия, которая сделает ее прозрачной и простой для верификаторов для оценки электронных транзакций. Обращаясь к разным авторитетам доверительных властей во всем мире и сочетая в себе доверительные аспекты, связанные с идентификацией, бизнесом, репутацией и т. д., станет возможным проводить доверительные решения для домена. Это достигается за счет повторного использования существующего управления, организации, инфраструктуры, стандартов, программного обеспечения, сообщества и ноу-хау существующей Системы доменных имен в сочетании с новыми инновационными строительными блоками. Такой подход позволяет эффективно проводить глобальное развертывание решения, которое помогает лицам, принимающим решения, принимать решения о доверии. Website: http://www.lightest.eu

PaaSword расширяет принципы облачной безопасности Cloud Security Alliance, используя последние инновации в технологиях промежуточного программного обеспечения виртуальной базы данных, которые внедряют масштабируемый уровень абстракции облачной базы данных облачных вычислений с использованием сложных методов распространения данных и шифрования. Реализация управления корпоративной безопасностью в облачных средах поддерживается новым подходом к контекстно-зависимым механизмам контроля доступа, которые включают динамически изменяющуюся контекстуальную информацию в политики контроля доступа и зависящие от контекста права доступа к данным, хранящимся в облаке. Наконец, PaaSword поддерживает разработчиков облачных приложений с помощью методов аннотации кода, которые позволяют указать соответствующий уровень защиты данных

приложения. Применимость, удобство использования, эффективность и ценность концепций PaaSword доказаны благодаря их интеграции в промышленные, реальные службы и приложения. Website: http://www.paasword.eu

KONFIDO - это проект H2020, целью которого является использование проверенных инструментов и процедур, а также новых подходов и передовых технологий с учетом создания масштабируемой и целостной парадигмы для безопасного внутреннего и трансграничного обмена, хранения и общей обработки данных здравоохранения юридически и этично, как на национальном, так и на европейском уровнях. Проект KONFIDO нацелен на продвижение новейшей технологии eHealth по четырем основным аспектам цифровой безопасности: сохранение данных, доступ к данным и их модификация, обмен данными и совместимость, соответствие требованиям. Практический подход KONFIDO основан на шести технологиях:

1. Новые расширения безопасности, предоставляемые некоторыми из основных поставщиков CPU (ЦП);
2. Решения безопасности на основе физической безоблачной функции (PUF), основанные на фотонных технологиях;
3. Гомоморфные механизмы шифрования;
4. Индивидуальные расширения выбранных решений безопасности и управления событиями (SIEM);
5. Набор механизмов разрушающего каротажа и аудита, разработанных в других технологических секторах, таких как blockchain, и перенесенных в область здравоохранения;
6. Индивидуальная реализация eIDAS-совместимого eID.

Website: http://www.konfido-project.eu

PANORAMIX - это проект ЕС H2020 по инновациям в области обеспечения конфиденциальности, предназначенный для обеспечения конфиденциальности через микс-сети. Это криптографическая настройка над существующими сетями, где помимо шифрования также удаляются мета-данные. Цель PANORAMIX - разработка многоцелевой инфраструктуры для обеспечения конфиденциальности, основанной на сетях микширования, и ее интеграции в высокоценные приложения, которые могут быть использованы европейскими компаниями. Три приложения, предназначенные для проекта, - это электронное голосование, статистика сохранения конфиденциальности и обмен сообщениями. Микс-сети защищают не только содержимое сообщений от третьих лиц, но также скрывают точную идентификацию отправителей или получателей сообщений с помощью криптографических реле. Микс-сети абсолютно необходимы для внедрения защищенных систем и протоколов, защищающих конфиденциальность. Website: https://panoramix-project.eu/

IV. Кибербезопасность в IoT

Основной целью, изложенной **GHOST** (Призрак), является разработка удобного для пользователя приложения для того, чтобы улучшить безопасность и конфиденциальность в цифровом доме, подключенном к Интернету вещей (IoT), используя самые передовые технологии, доступные для этой цели. Таким образом, Призрак будет способствовать росту европейского внутреннего рынка IoT, обеспечивая системы безопасности следующего поколения для домашних приложений (на основе таких технологий, как Blockchain или глубокий пакет инспекций) всем пользователям, независимо от их предыдущих знаний. С минимальными усилиями, потребители узнают и поймут риски кибер-безопасности (угрозы и уязвимости), и будут принимать информационные решения, влияющие на их кибер-физическую безопасность и конфиденциальность. GHOST поддерживается Рамочной программой ЕС по исследованиям и инновациям Horizon 2020. Десять компаний, организаций и университетов из шести стран являются частью проекта под руководством Televes. Website: https://www.ghost-iot.eu/

Проект **FORTIKA** направлен на предоставление МСП (малым предприятиям) встроенного, умного и надежного уровня безопасности оборудования улучшенного с помощью адаптивного управления службами экосистемы безопасности (база FORTIKA). В рамках проекта будут изучены возможности безопасной платформы FPGA SoC, как модуль повышения безопасности CPU (ЦП). Долгосрочная цель проекта FORTIKA - обеспечить недорогой динамический уровень безопасности для небольших компаний и предприятий среднего размера. Website: http://fortika-project.eu

Основной целью проекта **ANASTACIA** является решение проблем, связанных с кибер-безопасностью, посредство исследования, разработки и демонстрации целостного решения, обеспечивающего доверие и безопасности дизайна для кибер-физических систем (Cyber Physical Systems - CPS) на основе архитектур IoT и облаков (Cloud). ANASTACIA разработает надежную структуру безопасности, которая будет предусматривать все этапы жизненного цикла развития ИКТ-систем (SDL) и сможет принимать автономные решения с использованием новых сетевых технологий, таких как программно-конфигурируемые сети (SDN), виртуализация сетевых функций (NFV), интеллектуальная и динамические методологии, а также инструменты обеспечения безопасности и мониторинга. Website: http://www.anastacia-h2020.eu/

Основная цель **CIPSEC** - создать единую систему безопасности, которая организует новейшие разнородные продукты безопасности, обеспечивающие высокий уровень защиты в ИТ (информационные технологии) и ОТ (операционные технологии) отделов

CIs. Как часть этой структуры CIPSEC предложит полную экосистему безопасности дополнительных услуг, которые могут поддерживать предлагаемые технические решения для надежной и качественной работы. Эти услуги включают в себя тесты и рекомендации по уязвимостям, учебные курсы ключевому персоналу, государственно-частные партнерства (PPPs), судебно-медицинский анализ, стандартизация и защита от каскадных эффектов. Все решения и службы будут проверены в трех пилотах, выполняемых в трех разных средах CI (транспорт, здоровье и окружающая среда). CIPSEC также разработает маркетинговую стратегию для оптимального позиционирования его решения на рынке безопасности CI. Website: http://www.cipsec.eu/

ARMOR - это европейский проект (программа H2020), целью которого является решение вопросов безопасности и решение проблем в Интернете, предоставляя проверенные, оцененные и сертифицированные технологические решения (Security & Trust) для крупномасштабного IoT с использованием обновленных крупномасштабных тестов IoT / Cloud FIRE, оборудованных для экспериментов Security & Trust. ARMOR определила 3 цели, которые определяют подход, используемый для достижения предлагаемых решений в области безопасности и доверия:

• Усилить два развитых испытательных стенда FIRE с помощью экспериментальных инструментов ARMOR для обеспечения широкомасштабных экспериментов IoT Security & Trust;

• Реализовать шесть правильно проэкспериментированных, надлежащим образом проверенных и надлежащим образом оцененных методов и технологий для обеспечения безопасности и доверия в крупномасштабном IoT;

• Определить структуру для поддержки разработки приложений Secure & Trusted IoT, а также создать схему сертификации для установления уверенности в решениях безопасности и доверия IoT.

Website: https://www.armour-project.eu

Европейская система сертификации безопасности (**EU-SEC**) стремится решать проблемы безопасности, конфиденциальности и прозрачности, связанные с большим развитием облачных ИТ-сервисов. EU-SEC создаст систему сертификации, в рамках которой могут сосуществовать существующие схемы сертификации и обеспечения. Кроме того, в нем будет построена адаптированная архитектура и будет представлен набор инструментов для повышения эффективности и надежности существующих схем гарантии, предназначенных для обеспечения безопасности, управления, управления рисками и соответствия требованиям в Облаке. Она будет проверена и утверждена в пилотных проектах с участием промышленных партнеров. Website: https://www.recred.eu/

V. Кибербезопасность в социальных сетях

Появление социальных сетей привело к тому, что как компании, так и общественные организации стали чрезвычайно подвержены так называемой социальной инженерии 2.0 и, следовательно, подвержены целенаправленным кибер-атакам. К сожалению, в настоящее время на рынке нет решения, которое не позволяет ни всесторонней оценки социальных уязвимостей, ни управления и снижения связанного с ним риска. **DOGANA** стремится восполнить этот пробел, разработав структуру, которая обеспечивает «aDvanced sOcial enGineering And vulNerability Assessment». Основополагающая концепция DOGANA заключается в том, что оценки социальных рисков (SDVA), которые регулярно выполняются с помощью эффективных рамок, помогают развернуть эффективные стратегии смягчения последствий и привести к снижению риска, создаваемого современными методами атаки Social Engineering 2.0. Двумя соответствующими признаками предлагаемой структуры являются:

- наличие компонента «осведомленности» в рамках как краеугольного камня деятельности по предотвращению миграционной активности;
- правовые рамки по дизайну всей структуры, которая будет обеспечиваться партнером и рабочим пакетом, явно посвященным этой задаче.

Website: https://www.dogana-project.eu/

Общая цель проекта **ENCASE** заключается в том, чтобы использовать последние достижения в области безопасности и конфиденциальности несовершеннолетних (возраст 10-18 лет) для разработки и внедрения ориентированной на пользователя архитектуры для защиты несовершеннолетних от злонамеренных участников онлайн-социальных сетей (OSNs). Чтобы определить масштаб проблемы, ENCASE изучает существующие средства повышения безопасности и конфиденциальности, основанные на веб-инструментах, и проводит исследования, основанные на самых современных угрозах кибер-безопасности и безопасности в OSN. Более того, проект исследует проблему путем сбора данных из различных OSN.

ENCASE нацелена на разработку и внедрение платформы, которая сможет защитить несовершеннолетних и информировать их родителей, когда их дети подвергаются следующим угрозам в OSN:

1. Вредоносное поведение, кибер-запугивание и сексуальные домогательства
2. Ложное распространение информации и поддельная идентификация и деятельность
3. Чувствительное и обнаженное содержание.

Архитектура включает в себя три надстройки браузера, интеллектуальную веб-прокси-службу, которая будет отвечать за обнаружение вредоносного поведения, поддельных идентификаторов и активности и чувствительного контента в OSN на основе сложных правил обнаружения машинного обучения, созданных стеком программного обеспечения для анализа данных,

который является основой архитектуры. Website: http://encase.socialcomputing.eu/

VI. Кибер-безопасность в H2020

В течение следующих 48 месяцев эта система наблюдений (обсерватория) станет Европейским центром для кибер-безопасности и конфиденциальности. Мы будем следить за инициативами R & I по всему ЕС и Ассоциированным Странам, поддерживающим европейские заинтересованные стороны, которые играют активную роль в формировании глобального ландшафта кибер-безопасности и конфиденциальности. Благодаря сочетанию деятельности по кластеризации и уровню готовности к техническим и рыночным семинарам, будет отслеживаться весь жизненный цикл от разработки и исследований до внедрения, проверки и восприятия рынка, позволяя заинтересованным сторонам повысить их знания, повысить их осведомленность и найти возможный синергизм между различными инициативами. Website: https://www.cyberwatching.eu/

VII. Прочие разработки и платформы

SUNFISH предлагает услуги для объединения частных и общественных облаков, позволяющее им обмениваться данными и услугами безопасным и контролируемым образом, основанным на «демократической» модели управления: никакие правила федерации не действуют на других. Более подробно, SUNFISH разрабатывает дизайн и реализует «Федерация как услуга» (FaaS), облачное безопасное облако совместимости на основе технологии blockchain. Этот сервис реализуется через программную платформу под названием «SUNFISH Платформа", составляющие компоненты которой представляют собой существенные части от общего функционирования. Платформа SUNFISH является модульным программным решением, которое позволяет динамически и безопасно создавать облачные федерации и их управление. Ее основная функциональность: а) динамическое управление облаками; б) демократическое управление; с) безопасность данных. Проект SUNFISH разработал три конкретных примера развертывания, через три разных варианта использования. Website: http://www.sunfishproject.eu/

MF2C ставит перед собой задачу создать открытые, безопасные, децентрализованные, многосторонние системы управления заинтересованными сторонами, включая новые модели программирования, конфиденциальность и безопасность, методов хранения данных, создание сервисов, брокерские решения ,SLA и методы оркестровки ресурсов. Предполагается, что предлагаемая структура установит основы для новой архитектуры распределенной системы, доказательство концепции и платформы, подлежащих проверке и подтверждению в реальных случаях использования, как это предусмотрено для промышленных партнеров в консорциуме, быстрые инновации в секторе облачных вычислений. Website: http://www.mf2c-project.eu

WITDOM - это исследовательский проект, финансируемый ЕС Horizon 2020. WITDOM фокусируется на разработке инновационных решений для эффективных и практических методов повышения конфиденциальности и эффективной сигнальной и процессинговой обработки данных в зашифрованном домене для все более востребованных аутсорсинговых сред. На самом деле, главная цель WITDOM заключается в том, чтобы создать рамки для сквозной защиты данных в ненадежных и быстро меняющихся средах, основанных на ИКТ. Особый акцент делается на сценарии аутсорсинга данных, где появляются новые угрозы, уязвимости и риски, связанные с новыми потребностями, которые требуют комплексных решений безопасности, и которые будут выдерживать прогресс в течение всего срока службы поддерживаемых приложений. Website: http://witdom.eu/

YAKSHA стремится к укреплению сотрудничества между ЕС и АСЕАН и созданию партнерских отношений в области кибер-безопасности путем разработки решения, ориентированного на конкретные пользовательские и национальные потребности, используя ноу-хау ЕС и местный опыт. YAKSHA разработает и представит инновационную концепцию honeypots-as-a-service, которая значительно улучшит процесс сбора информации об угрозах. Это повысит уровень готовности кибер-безопасности для конечных пользователей, поможет предотвратить кибер-атаки, смягчит кибер-риски и улучшит управление всем процессом кибер-безопасности. YAKSHA идеально позиционируется для обеспечения глобальных цепочек поставок для производства, учитывая ее запланированное внимание к безопасности IoT. YAKSHA разработает инновационные методы обнаружения, сбора и анализа вредоносных программ, а также разработает специализированную онтологию, которая будет использоваться для долговременного хранения и анализа информации, для развертывания стандартных информационных форматов и интерфейсов для облегчения взаимодействия. Программное решение YAKSHA будет подтверждено в реальных экспериментальных проектах. Website: https://www.researchgate.net/project/YAKSHA

VIII. Заключение

Авторы, избрав эту манеру изложения, ставили себе целью представить наиболее выпукло то, с какими проблемами в области цифровой безопасности ЕС уже имеет дело, и то, как в Европе они решаются, чтобы была возможность подумать и поучиться, как это придется решать в России. Нам представляется, что поверхностные и упрощенные подходы в деле цифровой безопасности в нашей стране только вредят. Еще хуже, когда новые проблемы цифровой безопасности пытаются решить старыми аналоговыми способами.

Любознательный читатель, добравшийся до этой части статьи, может спросить: “Это весь перечень проектов ЕС по цифровой безопасности?” Ответ будет прост – нет. Заглянув на сайт Cyberwatching, этот читатель найдет еще множество проектов, описанных аналогичным образом (как в этой статье, но только на английском языке).

Нам представляется крайне важным сэкономить время российских исследователей и практиков, для того, чтобы они могли понять, как могут быть поставлены и решены в России проблемы цифровой безопасности наиболее оптимальными и быстрыми способами. Если это произойдет, то авторы будут считать свою задачу выполненной.

Библиография

[1] Указ Президента Российской Федерации «О Стратегии научно-технологического развития Российской Федерации « от 1 декабря 2016 года № 642

[2] Указ Президента Российской Федерации «О стратегии развития информационного общества в Российской Федерации» от 9 мая 2017 года № 2013

[3] Указ Президента Российской Федерации «О стратегии экономической безопасности Российской Федерации на период до 2030 года» от 13 мая 2017 года № 208

[4] Куприяновский В. П. и др. Правительство, промышленность, логистика, инновации и интеллектуальная мобильность в цифровой экономике //Современные информационные технологии и ИТ-образование. – 2017. – Т. 13. – №. 1 - С. 74-96

[5] Соколов И. А. и др. Цифровая безопасность умных городов //International Journal of Open Information Technologies. – 2018. – Т. 6. – №. 1. – С. 104-118.

[6] Покусаев О. Н. и др. Блокчейн на цифровой железной дороге Германии //International Journal of Open Information Technologies. – 2018. – Т. 6. – №. 2.- С. 43-53.

[7] Куприяновский В. П. и др. Развитие транспортно-логистических отраслей Европейского Союза: открытый BIM, Интернет Вещей и кибер-физические системы //International Journal of Open Information Technologies. – 2018. – Т. 6. – №. 2. – С. 54-100.

[8] Куприяновский В. П. и др. Мобильное производство на базе совместной экономики, цифровых технологий и логистики //International Journal of Open Information Technologies. – 2017. – Т. 5. – №. 8.

[9] Куприяновский В.П. и др. Гигабитное общество и инновации в цифровой экономике. //Современные информационные технологии и ИТ-образование 2017 Том 13 № 1. С. 106-129

[10] Kupriyanovsky V. et al. Intellectual mobility and mobility as a service in Smart Cities //International Journal of Open Information Technologies. – 2017. – Т. 5. – №. 12. – С. 77-122.

[11] Куприяновский В. П. и др. Aadhaar-идентификация человека в цифровой экономике //International Journal of Open Information Technologies. – 2017. – Т. 5. – №. 2.

[12] Namiot D. et al. Blockchain applications for transport industry //International Journal of Open Information Technologies. – 2017. – Т. 5. – №. 12. – С. 130-134.

[13] Deliverable D2.6 “Business and Technical Requirements (revised)” RECRED 26/07/2017 (184 стр.)

[14] Deliverable D2.7 “Reference architecture - revised” RECRED 27-07-2017 (98 стр.)

[15] D3.1 “Description of DCA protocols and technology support” RECRED Start Date May 1st, 2015 (74 стр.)

[16] Deliverable D3.2 “Multifactor authentication for DCA: user-todevice and device-to-network support” RECRED Start Date May 1st, 2015 (85 стр.)

[17] Deliverable D3.3 “Description of DCA protocols and technology support (revised)” RECRED 31/7/2017 (114 стр.)

[18] Deliverable D3.4 “Multifactor authentication for DCA: user-todevice and device-to-network support (revised)” RECRED Start Date May 1st, 2015 (50 стр.)

[19] Deliverable D4.1 “Identity Consolidator Baseline Platform” RECRED 2017-07-31 (91 стр.)

[20] Deliverable D4.2 “Full Identity Consolidator and Attributes Acquisition” RECRED 01-08-2017 (192 стр.)

[21] Deliverable D4.3 “Online identity and profile management” RECRED 2017-07-31 (73 стр.)

[22] Deliverable D5.1 “Specification and Initial Design of the ABAC Infrastructure” RECRED Start Date May 1st, 2015 (88 стр.)

[23] [1323] Deliverable D5.2 “Full Design and Prototype of the ABAC Infrastructure” RECRED 31/07/2017 (140 стр.)

[24] Deliverable 7.1 “HCI concept testing on user groups” RECRED 19.07.2017 (50 стр.)

[25] Deliverable D7.2 “Campus-wide Wi-Fi and web services access control pilot set up” RECRED Start Date May 1st, 2015 (60 стр.)

[26] Deliverable D7.3 “All Four Pilots Initial Setup & Progressing” RECRED 25/08/2017 (73 стр.)

[27] Deliverable D8.2 “Dissemination material including website” RECRED 31.07.2017 (16 стр.)

[28] Deliverable D8.3 “First dissemination report” RECRED 2017-07-31 (30 стр.)

[29] Deliverable D8.4 “Second dissemination report” RECRED 2017-07-31 (31 стр.).

Modern EU research projects and the digital security ontology of Europe

Igor Sokolov, Vasily Kupriyanovsky, Dmitry Namiot, Vladimir Sukhomlin, Oleg Pokusaev, Alexander Lavrov, Yuri Volokitin

***Abstract*— The article deals with issues related to cybersecurity in the digital economy. This paper provides a survey of research projects funded by the European Community, which address various issues of cybersecurity. The authors of the article believe that it will be useful for Russian researchers in this field to become familiar with the practice of the EU in this direction. Much attention is paid to the work on the creation of practical ontologies. Their results are published for wide discussion and practical use. The developed formal ontologies in artificial languages can be joined together and are designed to ensure the compatibility of data and applications, as well as their transparency throughout life cycles. It is the ontological approach that allows to calculate the basic control indicators of projects and, for example, to guarantee the fulfillment of the declared business rules.**

***Keywords*— cybersecurity, ontology, H2020.**