Некоторые вопросы концепции национальной безопасности в контексте глобальной цифровизации

Some aspects related to homeland security concept from the perspective of global digitalization

Осадчий / Osadchiy A.
Александр Иванович
(ai_osad@mail.ru)
доктор технических наук, профессор,
член-корреспондент РАЕН.
АО «Морэлектрорадиокомплект»,
генеральный директор.
г. Санкт-Петербург

Попов / Popov S.
Сергей Геннадьевич
(popovserge@spbstu.ru)
кандидат технических наук, доцент.
ФГАОУ ВО «Санкт-Петербургский политехнических университет Петра Великого»,
доцент кафедры «Телематика».
г. Санкт-Петербург

Осадчий / Osadchiy S.
Сергей Александрович
(spb.sos@hotmail.com)
АО «Морэлектрорадиокомплект»,
руководитель проекта.
г. Санкт-Петербург

Ключевые слова: национальная безопасность – homeland security; цифровая модель объекта – digital model of a facility; данные – data; программное обеспечение – software; формирование – generation; поиск – surveying; сбор – acquisition.

Бурное развитие Интернет-технологий и формирование большого массива данных (Big Data) в глобальных сетях привело к необходимости обеспечения национальной безопасности государства. В Российской Федерации в условиях санкций и импортозамещения иностранного оборудования и технологий возникает необходимость закрытия доступа к информации о разработке новых информационных и промышленных технологий в России. В статье предлагается подход к построению концептуальной модели национальной безопасности при формировании данных и цифровой модели объекта в контексте глобальной цифровизации.

Rapid development of Internet technologies and generation of data bulk in global networks resulted in the necessity to ensure homeland security. Due to sanctions and import substitution of foreign equipment and technologies in the Russian Federation it becomes necessary to block access to the data related to the development of new information and industrial technologies in Russia. The article offers an approach to building homeland security conceptual model for data generation and digital model of a facility from the perspective of global digitalization.

Современное развитие автоматизированных систем и искусственного интеллекта в рамках робототехники в настоящее время развивается без учета безопасности.

Бурное развитие автоматизированных систем и искусственного интеллекта может привести сначала к замене человека в быту и производстве, а затем и в системах управления. В дальнейшем развитие автоматизированных систем, робототехники и их программно-информационного обеспечения не исключают уничтожения современного уклада жизни человека, что может привести к серьезным последствиям, как в политической, так и экономической деятельности человечества во всем мире.

Эта аксиома должна заставить человечество задуматься об информационной безопасности в рамках развития цифровой экономики.

Создание ситуационных центров, автоматизированных систем электронного документооборота во всех сферах экономики и политики, от управления страной (министерства) до муниципального уровня (предприятия, банка), предполагают не только мониторинг, но и управление на основе больших данных, которые уже в настоящее время подвергаются все больше хакерским атакам.

Все это выставляет требование по информационной безопасности к процессу управления при разработке

и производстве различных систем управления во всех областях и сферах деятельности политики, экономики, промышленности, науки и техники.

Вопросы манипулирования и управления сознанием человека через встроенные ЧИПы и отпечатки пальцев со стороны автоматизированных систем, к чему это может привести! Уже сейчас современная молодежь со смартфоном или планшетом не расстается. Интернет и социальные сети типа «в контакте», «одноклассники» и другие просто «сжирают» время жизни человечества. В «твиттере» написал, эта фраза может касаться любого человека, занимающего пост от Президента и до рабочего. На рабочем месте человек с утра включает ПЭВМ, все рабочие места офисных работников оборудованы ПЭВМ.

В настоящее время существуют вызовы национальной безопасности в контексте глобальной цифровизации. Ведутся работы по разработке и созданию алгоритмов и технологий, которые позволяют извлекать некоторый контекст из всего объема больших данных (Big Data) и на его основе составлять цифровую модель объекта, представленную на рис. 1.

Технология должна «усиливать», «увеличивать», уточнять и расширять представление о цифровой модели объекта. При этом часть данных о цифровой модели объекта открытые, а часть данных закрытые.

В этой ситуации необходимо оценивать доступность к такой цифровой модели и ее влияние на национальную безопасность.

Если раньше шпионы охотились за документами и «торговали» документами, то в настоящее время охота идет за данными. А в условиях развития телекоммуникационных и социальных сетей национальной безопасности большей представляется угроза возможности хакерского программного обеспечения по доступу к закрытым данным, за счет развития технологий, алгоритмов по обработке открытых данных, а на их основе разработки программного обеспечения, умеющего формировать модели объекта за короткое время, пока информация не устарела и является актуальной исходя из целепологания.

Основу национальной безопасности составляют данные, которые могут быть не только открытыми и закрытыми, но и «краденными» [3]. Имеющиеся данные создают цифровую модель объекта, которая в свою очередь создает структуру программного обеспечения по формированию цифровой модели объекта (человек, процессор, автомобиль, самолет, вирус и т.д.).

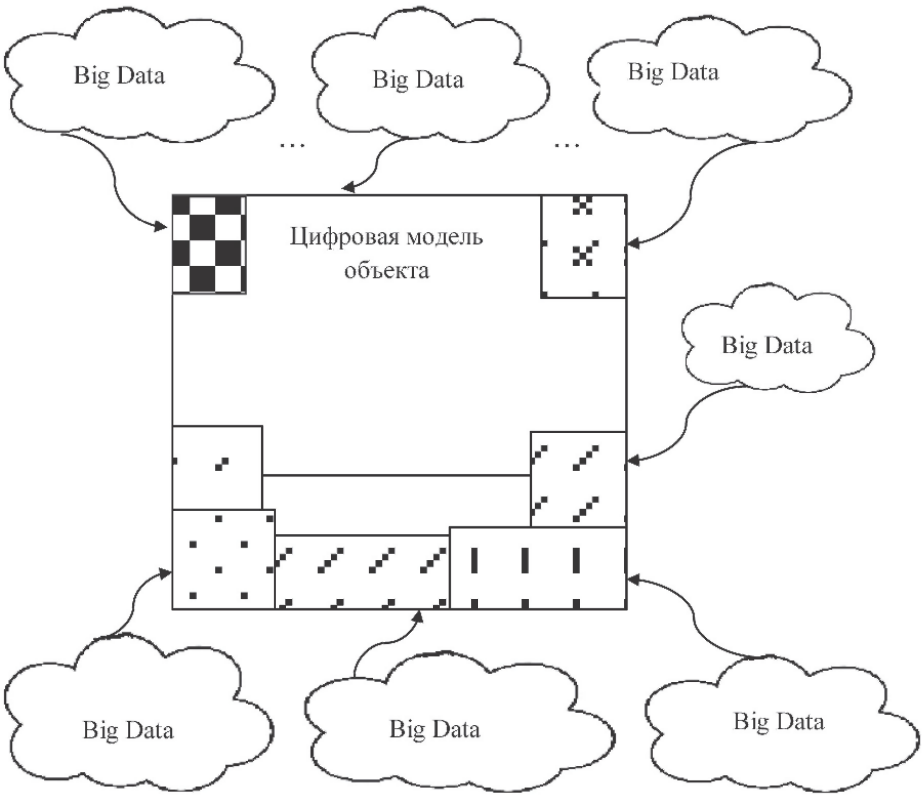

Рис. 1. Формирование цифровой модели объекта из Big Data

Программное обеспечение по формированию цифровой модели объекта должно быть универсальным.

Программное обеспечение должно уметь оценивать объем данных, которые можно собрать о цифровой модели объекта.

Программное обеспечение должно быть совместимо с технологией Big Data и обеспечивать автоматизированную обработку данных среди «хаоса» этих данных с целью формирования модели объекта.

Вызов национальной безопасности состоит в том, что структура программного обеспечения по цифровой модели объекта может сформировать структуру предприятий, занимающихся разработкой и производством, например самолета. При этом, имея цифровую модель объекта, можно оценить важность каждой детали, какое предприятие эту деталь делает, как остановить предприятие, затруднить работу и производство.

В этих условиях стоит задача обеспечения национальной безопасности государства по разработке новой технологии, которая могла бы динамически оценивать и затруднять извлекать некоторый контекст и на его основе составлять цифровую модель объекта.

Если раньше для решения задачи по поиску информации ставилась задача десяткам людей, которые осуществляли сбор информации, то в настоящее время национальной безопасности угрожает скорость сбора и обработки суперкомпьютерных технологий по формированию цифровой модели объекта.

Технология сбора и обработки данных по формированию цифровой модели объекта опирается на математические методы.

Поскольку формирование адекватной и достоверной цифровой модели объекта из множества данных является сложной технологической проблемой, для всего процесса должны применяться системный подход и системная методология [3]. Данный подход и методология при формировании облика и знаний о цифровой модели объекта трактует:

во-первых, в понимании цифровой модели объекта как системы (система – совокупность взаимосвязанных подсистем (элементов), обладающая интегративными и эмерджентными свойствами);

во-вторых, в понимании процесса исследования и поиска данных как системного по своей логике и применяемым средствам.

Во втором аспекте системный подход воплощает в жизнь требования диалектики по объективному, всестороннему и конкретному исследованию цифровой модели объекта, когда сочетаются методы индукции и дедукции, анализа и синтеза, идет постепенное и целенаправленное углубление в сущность рассматриваемой цифровой модели объекта, совершается восхождение от конкретного к абстрактному и далее – к целостному знанию. Первый и второй аспекты системного подхода выражаются в девяти основных принципах.

Процесс сбора и обработки связан с методами анализа и синтеза по определенным критериям, прописанным в программном обеспечении.

Поиск данных о цифровой модели объекта должен начинаться с выделения цифровой модели объекта из суперсистемы и изучение ее структуры. На данном этапе осуществляется определение состава цифровой модели объекта, состава среды и характеристик, а также внутренних и внешних связей. При правильном выделении системы из среды связи между элементами должны быть «сильнее», чем связи со средой.

Процесс выделения подсистем и элементов системы цифровой модели объекта и установление связей между ними принято называть структуризацией. При изучении структуры исследуются связи и класс сложности модели объекта в целом.

Глубина структуризации формирования данных о цифровой модели объекта зависит от значимости влияния элементов и подсистем, степени снятия неопределенности по каждому элементу, подсистеме и их взаимосвязи с другими элементами, подсистемами. При этом анализ возможен через синтез и наоборот синтез через анализ. В целом процесс анализа и синтеза при формировании адекватных и достоверных данных о цифровой модели объекта носит итеративный характер.

При формировании цифровой модели объекта прослеживаются три основных компонента системных исследований:

- структурный;
- функциональный;
- и исторический анализ, которые проводятся в строгом соответствии с целями поиска данных, выявленным предназначением цифровой модели объекта и с конечной целью формирования знаний о объекте (для разработки, создания и т. п.).

Основное отличие аналитического подхода от системного состоит в том, что при аналитическом подходе движение осуществляется от частей к целому, а при системном – от целого к частям и далее от частей к целому.

Процесс поиска и обработки данных требует рассматривать цифровую модель объекта как единое развивающееся целое, состоящее из взаимосвязанных частей и взаимодействующее с другими объектами, обладающими некоторыми недостающими данными для полного представления и пониманию самой модели объекта [3]. При этом данные о каждом элементе (подсистеме) цифровой модели объекта, как системы подвергается некоторым количественным и качественным изменениям, т.е. находится в развитии. Надо понимать, что цифровая модель объекта – это сложная система и имеет многоуровневую структуру, то есть подсистемы, элементы и данные. Межэлементные связи и данные об элементах являются наиболее важными системообразующими понятиями, благодаря которым формируется целостное знание и представление о цифровой модели объекта, которые позволяют приобрести эмерджентные

свойства. Цифровая модель объекта обладает не только эмерджентными, но и интегративными свойствами, которые не характерны элементам и данным о них.

В контексте глобальной цифровизации в рамках национальной безопасности, формируя открытый набор данных, необходимо оценивать безопасность публикаций с точки зрения глобальности, а не локальности. Например, данные водоканала (размещение коллекторов) и данные электросетей (трассы прокладки силовых кабелей к коллекторам), накладываем здания и видим узловые точки, мы создали цифровую модель объекта. Также можно делать выводы о личности. На сайте МВД есть паспортные данные, а в справке о доходах данные об объектах недвижимости, транспорте, финансовые и составе семьи, отсюда можно формировать выводы о личности, в настоящее время паспортные данные требуют везде, при этом просят расписаться о согласии на обработку персональных данных, а вот обеспечение их безопасности вызывает определенные вопросы, из чего можно сделать выводы об отсутствии реальной работы Закона о защите персональных данных (ФЗ-152).

Теоретически национальная безопасность должна осуществляться через программный продукт «экспертная система» с фильтрацией данных, перед тем как автор «выкладывает» в Big Data или передает данные по глобальным сетям на основе критериев, определенных в «экспертной системе». Формирование критериев должно опираться как на закон Российской Федерации « О Государственной тайне» №5485-1 от 21.07.1993, так и на Конституцию Российской Федерации от 12.12.1993 о доступности к информации.

Вопрос национальной безопасности в нашей стране «качнулся» в сторону открытости и доступности всех и ко всему в 90-е годы, а теперь нас «качнуло» в другую сторону – все закрыть. Истина должна быть посредине, не в области согласия, а в области компромиссов. Необходимо найти оптимум с разделением интересов гражданского общества и национальной безопасности государства, должен быть баланс между этими двумя частями. Возникает вопрос, как его формировать? Большинство правил устарело. В настоящее время со смартфона можно послать что угодно и куда угодно. В связи с этим видится, что правило, определенное в 40-е годы прошлого столетия, что секретоноситель не должен выезжать за границу, наверное устарело. Мы все туже завязываем мешок, а он дырявый. Утечка данных идет через глобальные сети, базы данных и Big Data.

Рассмотренные системные положения – это скорее всего схема формирования облика цифровой модели объекта, (методология) и, конечно, они не решают всех вопросов ее анализа и синтеза данных. Поэтому при создании технологии, алгоритмов, математических моделей, программного и информационного обеспечения необходимо принимать во внимание особенности реальных цифровых моделей объектов, процесса их функционирования с учетом конкретной среды.

При этом формирование данных и облика цифровой модели объекта в целом должно осуществляться по трем направлениям, с точки зрения:

1) процессов, протекающих как в цифровой модели объекта, так вне цифровой модели объекта (внешняя среда), но влияющих на данные о цифровой модели объекта;

2) цифровая модель объекта, которая состоит из данных о подсистемах (элементах), реализующих информационный процесс с учетом влияния внешней среды и суперсистемы;

3) управления цифровой моделью объекта, как суперсистемой для подсистем и элементов, в автоматическом режиме при автономной работе с учетом внутренних и внешних факторов.

Суть глобальной цифровизации – это появление в электронном пространстве цифровых моделей объектов.

Предмет национальной безопасности в противодействии создания целостного образа для этой цифровой модели объекта.

Это станет возможно, только когда в Российской Федерации будет обеспечен информационный суверенитет, который должен начинаться с создания отечественной элементной базы, операционной системы [1]. Операционная система должна обеспечивать режим «симплекса» при работе абонента в системе и доступ из внешней среды должен осуществляться по разрешению абонента. При наличии отечественной элементной базы можно будет разрабатывать и производить системы: маршрутизации, коммутации, межсетевые экраны, серверное оборудование, ПЭВМ и другое телекоммуникационное оборудование, с помощью которого будет обеспечиваться национальная безопасность при глобальной цифровизации, в том числе цифровой экономики [2]. Для этого должна быть создана ФЦП и корпорация в каждом Министерстве, с руководителя которого можно будет спросить за результаты. Корпорация должна включать в себя ВУЗы, предприятия, имеющие опыт, желание и научный задел в направлении создания отечественной элементной базы. Дать возможность в этом направлении осуществлять разработку отечественной элементной базы ВУЗам РФ, в том числе отраслевым, а не только предприятиям.

Финансирование ФЦП по разработке отечественной элементной базы должны осуществлять:

– министерство промышленности и торговли;
– министерство образования;
– минкомсвязи.

При этом целесообразным видится не включать в этот список предприятия, которым были выделены средства на разработку отечественной элементной базы и программного обеспечения, но которые не достигли положительных результатов.

Таким образом, в условиях глобальной цифровизации и нарастающей агрессии НАТО, киберагрессии и атак, внедрении в состав систем управления зарубежных

операционных систем, программного обеспечения и телекоммуникационного оборудования, не обеспечивающих несанкционированный доступ и недекларированные возможности, необходимо:

1. Создание в России ведущего Федерального центра информационных технологий и кибербезопасности (ФЦИТиК) как стратегического партнера развития и внедрения фундаментальных, опережающих информационных технологий и на этой основе создание отечественной высокотехнологичной промышленности телекоммуникационного оборудования и подготовки высококвалифицированных кадров для отрасли.

2. Создание на Северо-Западе России кластера инфотелекоммуникационных технологий и кибербезопасности (ИТКиК)– как основы развития сетей связи двойного назначения.

3. Сохранение отрасли связи и подъем отрасли на новый технологический уровень.

4. Обеспечение безопасности систем управления, органов государственного управления и силовых структур на основе построения сетей связи на высокотехнологичном отечественном оборудовании.

5. Замена импортного оборудования на сетях связи общего пользования с 90 % в настоящее время и доведение наличия импортного оборудования на сетях связи операторов связи до 25 % с 2019 года до 2025 года.

6. Исключение импортного оборудования на сетях связи органов власти и силовых структур.

Основа создания Федерального центра информационных технологий и кибербезопасности в России Указ Президента РФ №899 от 7 июля 2011г. «Об утверждении приоритетных направлений развития науки, технологий и техники в РФ и перечня критических технологий РФ» одно из Приоритетных направлений под №3 – Информационно-телекоммуникационные системы.

Необходимость создания ФЦИТиК опирается на разработанную стратегию для реализации «Основных направлений государственной политики в области развития систем связи для нужд обороны страны, безопасности государства и поддержания правопорядка на период до 2020 года» и состояние дел в отрасли (в области производства отечественного оборудования и подготовки кадров).

Литература

1. Осадчий, А. И. Трансфер телекоммуникационных технологий / А.И. Осадчий, В.И. Комашинский, Т.А. Блатова // Вестник связи. – 2012. – № 8. – С. 16–19.

2. Анализ состояния телекоммуникационных сетей сети связи общего пользования и целесообразности их использования в интересах сетей связи специального назначения / А.И. Осадчий [и др.]. – Научно-технический сборник № 2 (4). – М.: ОАО «Концерн «Системпром», 2013. – С. 270–274.

3. Обеспечение устойчивости информационно-телекоммуникационных сетей в условиях информационного противоборства / М.А. Коцыняк [и др.]. – СПб: ЛО ЦНИИС, 2014. – 126 с.