ИНТЕРОПЕРАБЕЛЬНОСТЬ КАК ОСНОВА ДЛЯ СИСТЕМАТИЗАЦИИ МЕТОДОВ И СРЕДСТВ ИНФОРМАЦИОННОЙ БЕЗОПАСНОСТИ

Гришенцев А. Ю.[1], Коровкин Н. В.[2], Коробейников А. Г.[3]

DOI: 10.21681/2311-3456-2025-5-15-27

Цель исследования: *развитие теоретических основ информационной безопасности за счёт обоснованной систематизации, методов и средств информационной безопасности на основе понятия интероперабельность.*

Методы исследования: *анализ информационного взаимодействия и угроз при информационном взаимодействии на основе стандартизированной эталонной модели интероперабельности и синтез систематической структурированной модели методов и средств информационной безопасности в контексте понятия интероперабельность.*

Результаты исследования: *на основе анализа научных направлений интероперабельность и информационная безопасность, предлагается дополнить область интересов информационной безопасности семантическим уровнем, в соответствии с эталонной моделью интероперабельности. Выполнен анализ угроз информационной безопасности объекту защиты реализуемых на семантическом уровне информационного взаимодействия. В ходе исследований доказана необходимость информационной безопасности на семантическом уровне для обеспечения полноты защиты информационного взаимодействия и удовлетворения интересов объекта информационной защиты. Предложена информационная модель разработки и реализации методов информационной безопасности способствующая достижению целей объекта защиты. Предложена модель информационной безопасности на основе эталонной модели интероперабельности. Предложена модель аудита и оценки рисков информационной безопасности на основе эталонной модели интероперабельности.*

Научная новизна: *заключается в новом подходе к систематизации методов, средств и увеличении сферы интересов информационной безопасности на основе современных научных представлений о уровнях информационного взаимодействия в соответствии с понятием интероперабельность.*

Ключевые слова: *защита информации, информационное взаимодействие, открытые системы, модели, стандарты.*

Введение

Отечественный ГОСТ по основным терминам и определениям интероперабельности с 2012 года обновился дважды, первое издание 2012 года ГОСТ Р 55062–2012[4], второе, обновлённое, дополненное и переработанное, 2021 года ГОСТ Р 55062–2021[5].

В соответствии с ГОСТ Р 55062–2021, интероперабельность – способность двух или более информационных систем (ИС) или компонентов к обмену информацией и к использованию информации, полученной в результате обмена.

Значительным фактором эволюции научного знания являются благоприятные условия внешней среды, стимулирующие развитие. Для информационной безопасности благоприятными факторами внешней среды, являются: интерес различных лиц и организаций к её проблемам и высокий спрос на специалистов. Но, пожалуй, основным фактором является постановка приоритетов развития и обозначение имеющихся преград и препятствий на государственном уровне. Так на заседании дискуссионного клуба «Валдай» [1] которое состоялось 7 ноября 2024 в Сочи, в речи президента РФ В. В. Путина впервые на высшем уровне озвучен факт не суверенного положения РФ, обозначен приоритет борьбы за суверенитет и отмечена ключевая роль и комплексность понятия безопасности.

По мнению авторов, актуальность исследований поддержана создавшимися политическими и экономическими условиями, сложившимися в настоящее время внутри Российской Федерации и за её рубежами.

1 Гришенцев Алексей Юрьевич, доктор технических наук, доцент, член-корреспондент Академии электротехнических наук Российской Федерации, доцент Федерального государственного автономного образовательного учреждения высшего образования Национальный исследовательский университет ИТМО. Санкт Петербург, Россия. E-mail: AGrishentsev@yandex.ru

2 Коровкин Николай Владимирович, доктор технических наук, профессор, действительный член Академии Электротехнических Наук Российской Федерации, профессор Федерального государственного автономного образовательного учреждения высшего образования Санкт Петербургский политехнический университет Петра Великого. Санкт-Петербург, Россия. E-mail: Nikolay.Korovkin@gmail.com

3 Коробейников Анатолий Григорьевич, доктор технических наук, профессор, заместитель директора по науке Санкт-Петербургского филиала Федерального государственного бюджетного учреждения науки Института земного магнетизма, ионосферы и распространения радиоволн им. Н. В. Пушкова Российской академии наук, профессор Федерального государственного автономного образовательного учреждения высшего образования Национальный исследовательский университет ИТМО. Санкт-Петербург, Россия. E-mail: Korobeynikov_A_G@mail.ru

4 ГОСТ Р 55062–2012 Информационные технологии. Системы промышленной автоматизации и их интеграция. Интероперабельность. Основные положения. М.: Стандартинформ, 2012. – 11 с.

5 ГОСТ Р 55062–2021 Информационные технологии. Интероперабельность. Основные положения. М.: Стандартинформ, 2021. – 11 с.

В частности вектором развития, о котором идёт немало дискуссий, в том числе в научных работах и верхних эшелонах власти, направленным на технологический и производственный суверенитет [2] в условиях санкционного давления и мирового системного кризиса, охватывающего все сферы интересов человеческой цивилизации от политического и экономического до культурного, демографического и миграционного [3]. Таким образом, актуальным является выявление угроз и обеспечение информационной безопасности на всех уровнях информационного взаимодействия информационных систем и/или их компонентов.

Состояние исследований по интероперабельности и предпосылки к постановке задачи

Впервые необходимость систематизации информационного взаимодействия в рамках понятия интероперабельность сформировалась в недрах военных ведомств[6] США и промышленных гигантов[7] в области информационных технологий. В частности, одно из первых определений интероперабельности дано министерством обороны США[8] (англ. Department of Defense, US DOD). В этом же документе, со ссылкой на (Electronic Warfare. Joint Pub. 3-13.1) даётся определение понятия информации. Информация – 1) факты, данные или инструкции в любом виде; 2) значение, которое человек придает данным с помощью известных соглашений, используемых при их представлении. Приведём точные формулировки на английском. Information – 1) Facts, data, or instructions in any medium or form. 2) The meaning that a human assigns to data by means of the known conventions used in their representation (JP 3-13.1). В части 2 определения информации подчёркивается значимость семантического уровня информационных взаимодействий, т.е. известных соглашений (о смыслах), и разделение собственно данных и информации на две различных понятийных категории. При этом в первом определении информации факты, данные или инструкции, являются её синонимами. По мнению авторов, второе определение понятия информации является более полным, т.к. ключевым аспектом информационной интерпретации тех или иных данных, фактов, инструкций является их смысловое наполнение, что достигается за счёт соглашений о смыслах.

Имеется немало отечественных публикаций о функции информационного взаимодействия в процессе управления и эволюции информационных систем [4–6], а также о вопросах безопасности информационного взаимодействия и противоборства [7–9]. При этом отсутствуют работы в явном виде, связывающие модель информационного взаимодействия на основе понятия интероперабельность и информационную безопасность.

Из определения интероперабельности ясно, что интероперабельность занимается систематизацией и исследованием способности к информационным отношениям между системами или их элементами техническими [10, 11], а также и/или биологическими, например, в виде человеко-машинных интерфейсов в промышленности и науке [12, 13] в медицине [14]. В свою очередь, информационная безопасность, как сказано в ряде различных трудов [15] и нормативных документов, например: ГОСТ Р 53114-2008, ГОСТ Р 50922-2006, занимается защитой интересов объектов (и субъектов) информационного взаимодействия, которые так же являются информационными системами. Следовательно, уровни информационного взаимодействия интероперабельности, по мнению авторов, могут и должны являться основой для систематизации методов и средств информационной безопасности и защиты информации. Это обоснованно тем, что информационная безопасность защищает интересы некоторой стороны информационного взаимодействия, а само информационное взаимодействие, как доказывает теория и практика развития интероперабельности происходит на уровнях, называемых уровни интероперабельности [16].

В рамках данной работы предлагается использовать интероперабельность как основу для систематизации методов и средств информационной безопасности.

Ещё одной предпосылкой к данному исследованию является то, что некоторые специалисты по информационной безопасности позиционируют информационную безопасность как методы защиты информации безразличные к её сущности и содержанию. На некоторых уровнях информационной безопасности такой подход приемлем и даже необходим, но не достаточен для реализации информационной безопасности как надёжного инструмента, обеспечивающего защиту интересов объектов информационного взаимодействия от отдельного гражданина до государства и цивилизации в целом.

Модель интероперабельности и информационная безопасность

Эталонная модель интероперабельности (ГОСТ Р 55062–2021), приведенная на рисунке 1, представляет собой развитие семиуровневой базовой эталонной модели взаимосвязи открытых систем (ВОС) согласно ГОСТ Р ИСО/МЭК 7498-1, и образована тремя уровнями: техническим, семантическим и организационным.

6 Department of Defense Dictionary of Military and Associated Terms. Joint Pub. 1-02. 1994. – 633 p.

7 Handley M., Schulzrinne H., Schooler E., Rosenberg J. SIP: Session Initiation Protocol. Network Working Group. 1999. RFC 2453. URL: https://www.ietf.org/rfc/rfc2543.txt (date of request: 16.05.2025).

8 Department of Defense Dictionary of Military and Associated Terms. Joint Pub. 1-02. 1994, as amended through 10 january 2000 URL: https://www.bits.de/NRANEU/others/jp-doctrine/jp1_02(00).pdf (date of request: 16.05.2025).

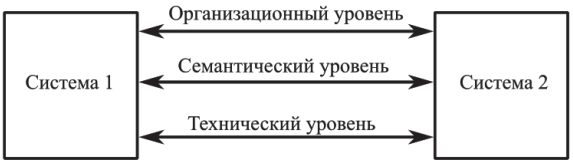

Рис. 1. Эталонная модель интероперабельности

Технический уровень – описывает синтаксис или форматы передаваемой информации, заостряя внимание на том, как представлена информация в коммуникационной среде. Технический уровень включает такие ключевые аспекты, как открытые интерфейсы, службы связи, интеграция данных и промежуточный слой программного обеспечения (Middleware), представление и обмен данными, службы доступности и защиты информации. Техническая интероперабельность достигается главным образом за счет использования стандартных протоколов связи типа TCP/IP.

Семантический уровень – описывает семантические аспекты взаимодействия, т. е. содержательную сторону информационного обмена. Семантическая интероперабельность позволяет системам комбинировать полученную информацию с другими информационными ресурсами и обрабатывать ее смысловое содержание. Семантическая интероперабельность достигается за счет применения стандартов типа XML (XSD, RDF, OWL).

Организационный уровень – акцентирует внимание на прагматических аспектах взаимодействия (деловых или политических). На этом уровне согласуются бизнес-цели и достигаются соглашения о сотрудничестве между административными органами, которые хотят обмениваться информацией, хотя имеют отличающиеся внутреннюю структуру и процессы. Организационная интероперабельность имеет своей целью удовлетворить требования сообщества пользователей: службы должны стать доступными, легко идентифицироваться, и быть ориентированными на пользователя. Организационная интероперабельность достигается не за счет применения стандартов (нормативно-технических документов), а за счет применения нормативно-правовых документов (соглашений, конвенций, договоров о сотрудничестве).

По отношению к объекту информационного взаимодействия различают внешнюю и внутреннюю интероперабельность. В ГОСТ Р 55062–2021 даны следующее определения:

- внешняя интероперабельность предприятия (external enterprise interoperability) – интероперабельность, которая определяет взаимодействие предприятия с другими предприятиями и конкурентоспособность предприятия на рынке;
- внутренняя интероперабельность предприятия (internal enterprise interoperability) – интероперабельность внутренней инфраструктуры (корпоративной системы) предприятия.

И дополнительно отметим, как в ГОСТ Р 55062–2021 определена интероперабельность предприятия (enterprise interoperability) – способность предприятий или находящихся в них сущностей (объектов) осуществлять эффективную связь и взаимодействие.

Эталонная модель интероперабельности предлагает разделение эффективного информационного взаимодействия на три уровня (рис. 1). Исследуем следующий вопрос: все ли уровни этого взаимодействия для реализации защиты интересов объектов и субъектов информационных отношений охватывает информационная безопасность, в том виде, в каком она позиционируется некоторыми экспертами и рядом нормативных документов?

Для поиска ответа на поставленный вопрос произведём сопоставление уровней определённых для интероперабельности с видами защиты информации определёнными в ГОСТ Р 50922-2006.

Правовая защита информации – защита информации правовыми методами, включающая в себя разработку законодательных и нормативных правовых документов (актов), регулирующих отношения субъектов по защите информации, применение этих документов (актов), а также надзор и контроль за их исполнением.

Техническая защита информации (ТЗИ) – защита информации, заключающаяся в обеспечении не криптографическими методами безопасности информации (данных), подлежащей (подлежащих) защите в соответствии с действующим законодательством, с применением технических, программных и программно-технических средств.

Криптографическая защита информации – защита информации с помощью ее криптографического преобразования.

Физическая защита информации – защита информации путем применения организационных мероприятий и совокупности средств, создающих препятствия для проникновения или доступа неуполномоченных физических лиц к объекту защиты.

Анализ показывает, виды информационной безопасности не включают семантический уровень информационного взаимодействия. Техническая, криптографическая и физическая защита информации относится к техническому уровню информационного взаимодействия, работа на техническом уровне информационной безопасности, во многих, но не во всех случаях, может вестись без учёта смысловой нагрузки защищаемой информации. Правовая защита информации относится к организационному

уровню, т.к. организационный уровень интероперабельности акцентирует внимание на прагматических аспектах взаимодействия (деловых или политических, и в том числе правовых). И надо отметить, что правовой уровень защиты информации не обходится без семантического, т.к. сама функция права не может быть реализована без вложения в право смысла. Поэтому, в неявном виде семантический уровень информационной безопасности имеется, но в явном виде, в виде, определяющем область научных интересов информационной безопасности – отсутствует.

Семантический уровень

Семантический уровень иначе уровень смыслов, в общем случае является ключевым для возможности реализации и обеспечения интересов и защиты сторон при информационном взаимодействии. Уровень смыслов необходим не только для внешнего межсистемного взаимодействия, но и для информационного взаимодействия внутри системы. Уровень смыслов определяет трактовку тех или иных частных и общих договорённостей, сообщений, соглашений. Самая значительная возможность семантического уровня это синтез новых смыслов и критический аудит имеющихся с целью повышения содержательной сути, а значит повышения качества информационного взаимодействия. В информационном межсистемном взаимодействии, побеждают более сильные идеи и смыслы, которые и определяют ход дальнейшей эволюции. Поэтому столь значима борьба за доминирование одних идей над другими. Так при колонизации метрополии навязывают свои смыслы и идеи колониям, как в период, предшествующий колонизации, так и после, для удержания статуса метрополии. Доминирующие на рынке компании определяют ценовую политику и способны регулировать спрос за счёт социальной инженерии, рекламы, лоббирования своих интересов в государственных органах управления и пр., тем самым навязывая свои идеи и смыслы социальным системам (рынкам) различного масштаба.

Один из способов оценки эффективности функционирования системы в условиях агрессивной внешней среды, основан на показателях скорости и точности достижения поставленной цели. Для социальных систем, цели, т.е. смыслы существования мотивы к развитию, обычно трансформируются в идеологию, задающую общий вектор развития и поддержанный отдельными частными целями и способствующими их достижению задачами. При отсутствии явно сформулированной цели, определяющей вектор движения системы, невозможно оценить эффективность движения, или наоборот можно дать любую оценку произвольному движению или топтанию на месте. А если такая цель не поставлена явно или сформулирована расплывчато, то означает ли это, что такой цели нет? Нет, не означает. Во-первых, у субъекта хозяйствования может иметься цель, но она не формулируется явно внутренними агентами или подменяется иными целями, не соответствующими реальным. Подмена цели обычно является следствием того, что фактическая цель является плохим мотиватором для элементов системы и потому не формулируется явно внутренними агентами системы. Во-вторых, цель для объекта, не имеющего собственной цели, будет поставлена из внешнего пространства. Следует отметить, что наличие собственной цели не гарантирует защиту от постановки внешней цели. Особенно, если в качестве объектов рассматривать достаточно крупные объекты хозяйственно-экономической деятельности как внутри отдельной страны, так и на международной арене. Понятно, что такие объекты, не имеющие собственной цели или имеющие слабую цель, в условиях борьбы за различные ресурсы не останутся без внимания других объектов и субъектов хозяйствования. Поэтому имеются основания полагать, что цель для объекта, не имеющего собственной цели или имеющего слабую цель, будет поставлена из внешнего пространства внешними субъектами, имеющими более сильную цель и располагающими ресурсами для её реализации. Так же имеются предпосылки полагать, что такая, внешняя, цель не всегда будет воспринята как действующий эффективный мотиватор для участников рассматриваемой системы и потому не формулируется явно внутренними управляющими агентами системы. Постановка цели внешними объектами и субъектами информационного взаимодействия и принуждение к её достижению может быть реализовано с помощью различных инструментов, в том числе инструментов манипуляции и принуждения (экономических, социо-психологических, политических, правовых, военных и др.), и так или иначе принуждая объект, не имеющий собственной цели или имеющий собственную слабую цель, действовать в соответствии с целями чужими.

Целевым концентратом, т.е. обобщением частных целей и задач всех государственных и действующих в правовом поле государства объектов можно назвать идеологию. Здесь уместно отметить Статью 13, часть 2 Конституции РФ «Никакая идеология не может устанавливаться в качестве государственной или обязательной» с учётом речи В. В. Путина на заседании дискуссионного клуба «Валдай» [1] в которой явного сказано о борьбе за суверенитет России. Отсутствие государственной идеологии есть прямое указание к отсутствию собственной цели государства.

Постановка цели внешними субъектами информационного взаимодействия далеко не всегда является деструктивным фактором для системы, в той или

иной степени находящейся под внешним управлением. Например, объекты хозяйственно-экономической деятельности, действующие в правовом поле на территории определённого государства, вынуждены соблюдать установленные внутри этого государства законы, а отдельное предприятие, ведущее свою деятельность в составе корпорации, выполняет задачи, поставленные корпорацией. В общем случае при информационном взаимодействии все вовлечённые объекты и субъекты в той или иной степени ограничены в реализации собственных целей, в предельном случае таким ограничителем являются законы природы (включая законы физические, экономические, социальные и пр). Если объекты претендуют на равноправие в построении информационных, экономических и прочих отношений, то цели, требующие общего участия сторон, должны быть выработаны как обоюдовыгодный компромисс. Причём степень уступок в компромиссе и определяется степенью принуждения со стороны бенефициара данных уступок. Эволюция цивилизации показывает, что процесс глобализации является неизбежным, и вероятно является законом развития сложных социальных систем, в условиях, глобализации смысл понятия «суверенитет» значительно отличается от смысла «суверенитета» в цивилизационный период до глобализации. Вот, например, президент «мирового гегемона» США и вероятно некоторая значительная часть его избирателей, считают, что США не имеют независимости и суверенитета, о чем можно сделать вывод из инаугурационной речи Д. Трампа: «Наш суверенитет будет восстановлен. Наша безопасность будет восстановлена… С этого дня Соединенные Штаты Америки будут свободной, суверенной и независимой нацией.» [17]. Вероятно, одним из самых значимых факторов суверенитета в современном мире, идущем по пути глобализации, является производственно-технологический суверенитет, о чём в той же речи говорит Д. Трамп: «Америка снова станет страной-производителем, и у нас есть то, чего никогда не будет ни у одной другой страны-производителя, – крупнейшие в мире запасы нефти и газа, и мы собираемся использовать их. Мы будем их использовать.» [17].

Определение уровня уступок и компромисса в условиях неизбежной глобализации является отдельной проблемой, которую необходимо исследовать и решать, в том числе на основе информационной безопасности с учётом всех уровней информационного взаимодействия.

Если говорить о человеческой цивилизации, в современном её состоянии, то распределение смыслов по значимости можно представить следующей моделью: смыслы, генерируемые цивилизацией в целом, т.е. совокупностью всех образующих цивилизацию объектов и субъектов, такие смыслы по модели В. И. Вернадского можно ассоциировать с некоторым планетарным явлением – ноосфера [18]; далее надгосударственные структуры, не отвечающие по обязательствам государств, но способные влиять на постановку целей государствами, например, Федеральная резервная система [19, 20]; отдельные государства; далее структуры в составе государства, коллективы и общественные организации; далее семья и отдельный человек. Нельзя сказать, что с точки зрения отдельного человека уровень смыслов, не имеет никакого значения, напротив, для развитого человека, реализующего свой творческий потенциал, цель жизни может быть основным мотиватором и двигателем его созидательного или разрушительного начала. Примером, формирования, развития смыслов и идей может быть жизнь и труд авиаконструктора Александра Сергеевича Яковлева [21], предпринимателя Генри Форда [22], учёного-электротехника Владимира Фёдоровича Мицкевича [23, 24] и др.; надо сказать – примеров постановки цели личностью и решительного стремления к ней немало в истории человечества. И не всегда эти цели были созидательные. Но раз в самом низу пирамиды целей и смыслов цель имеет столь великую силу, то ещё большую силу может иметь цель коллективная «Идеи становятся материальной силой, когда они овладевают массами» (К. Маркс). Таким образом, для всех перечисленных выше системных уровней цивилизации необходимы смыслы и цель, в первую очередь для эффективного и безопасного информационного взаимодействия, при котором на необходимый и достаточный уровень информационной безопасности могут рассчитывать все участники. При такой постановке вопроса информационная безопасность в соответствии с эталонной моделью интероперабельности можно так же подразделить на: техническую, семантическую и организационную.

Исследования в области интероперабельности, убедительно показывают, что информационное взаимодействие включает уровень смыслов, т.е. семантический уровень. Информационная безопасность, будучи не только техническим инструментом, но и научным направлением (о чем, например, говорят две научные специальности по номенклатуре ВАК: 2.3.6 Методы и системы защиты информации, информационная безопасность и 1.2.4 Кибербезопасность), должна систематически исследовать вопрос обеспечения интересов защищаемой стороны информационного взаимодействия, что означает исследовать угрозы информационного взаимодействия на всех уровнях: техническом, семантическом, организационном. Вероятно, не каждый специалист по информационной безопасности должен непосредственно заниматься совершенствованием

семантического и/или правого уровня информационной безопасности, но, по мнению авторов, каждый специалист по информационной безопасности, должен знать и понимать, что современная теория информационного взаимодействия основана на модели интероперабельности. Это, например, определяет особенности построения учебных программ для студентов и аспирантов соответствующих специальностей.

Информационная модель обеспечения безопасности

На основе приведённых рассуждений сформируем концепт обеспечения информационной безопасности объекта защиты. По мнению авторов, наиболее значимой задачей информационной безопасности является формирование и аудит целей, т.е. эволюции объекта защиты в условиях агрессивной среды. Следует различать средства и методы обеспечения информационного взаимодействия внутри объекта защиты, т.е. внутренние, и средства и методы обеспечения информационной безопасности за периметром объекта защиты, т.е. внешние. Цели объекта защиты формируются на будущее время, поэтому необходимо иметь прогноз, как о состоянии внешней среды, так и об изменении ресурсов и потенциала объекта защиты. Причём время прогнозирования должно быть достаточным для постановки и реализации тактических и стратегических целей, адекватных внешним условиям и собственному потенциалу объекта защиты. Современная физика придерживается той модели, при которой физический объект оказывает некоторое возмущение на окружающую его внешнюю среду, а внешняя среда на объект. При информационном взаимодействии с внешней средой объект защиты так же оказывает влияние на внешнюю среду, а внешняя среда воздействует на объект защиты. Поэтому цели объекта защиты должны быть такими, что бы производимые им возмущения внешней среды создавали наиболее благоприятные условия для реализации поставленных целей. С другой стороны необходимо минимизировать возмущающее воздействие внешней среды на объект защиты, препятствующее достижению целей объекта защиты.

Собственное (т.е. внутреннее) состояние объекта защиты так же должно способствовать достижению поставленной цели. Фактически любой информационный субъект, являющийся частью объекта защиты, оказывает возмущающее воздействие на другие частные информационные субъекты объекта, следовательно, на состояние объекта в целом. Поэтому необходим мониторинг, аудит и обеспечение информационной безопасности внутреннего информационного взаимодействия объекта защиты.

Условия внешней среды и состояние объекта защиты, являются не стационарными, но динамическими, т.е. изменяющимися с течением времени, поэтому для реализации эффективного и адекватного управления необходим мониторинг внешней среды и состояния объекта защиты, и своевременная корректировка информационного управляющего воздействия, т.е. корректировка положения объекта защиты в пространстве возможных состояний [25, 26].

Отметим, что не всё информационное взаимодействие сколько-нибудь сложного объекта защиты может наблюдаться средствами и методами информационной безопасности. Ещё меньшая часть информационного взаимодействия может управляться с применением методов информационной безопасности. Такие обстоятельства могут значительно затруднить реализацию информационной безопасности объекта защиты. А само информационное взаимодействие можно отобразить в виде диаграммы Эйлера-Вена (рис. 2).

Ранее было сказано, что основная функция, реализуемая при информационном взаимодействии – управление. Следовательно, более развёрнутая формулировка задачи информационной безопасности – определение целей объекта защиты и информационной безопасности объекта, обеспечение эффективного управления объектом защиты за счёт безопасности внутреннего и внешнего информационного взаимодействия на всех уровнях интероперабельности для достижения поставленной объектом цели.

Оценка управления осуществляется на основании оценки достижения поставленных целей. Следовательно, оценка информационной безопасности,

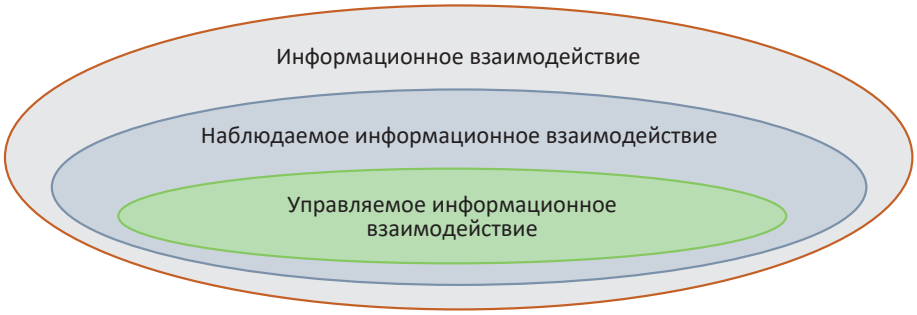

Рис. 2. Наблюдаемое и управляемое в общем информационном взаимодействии

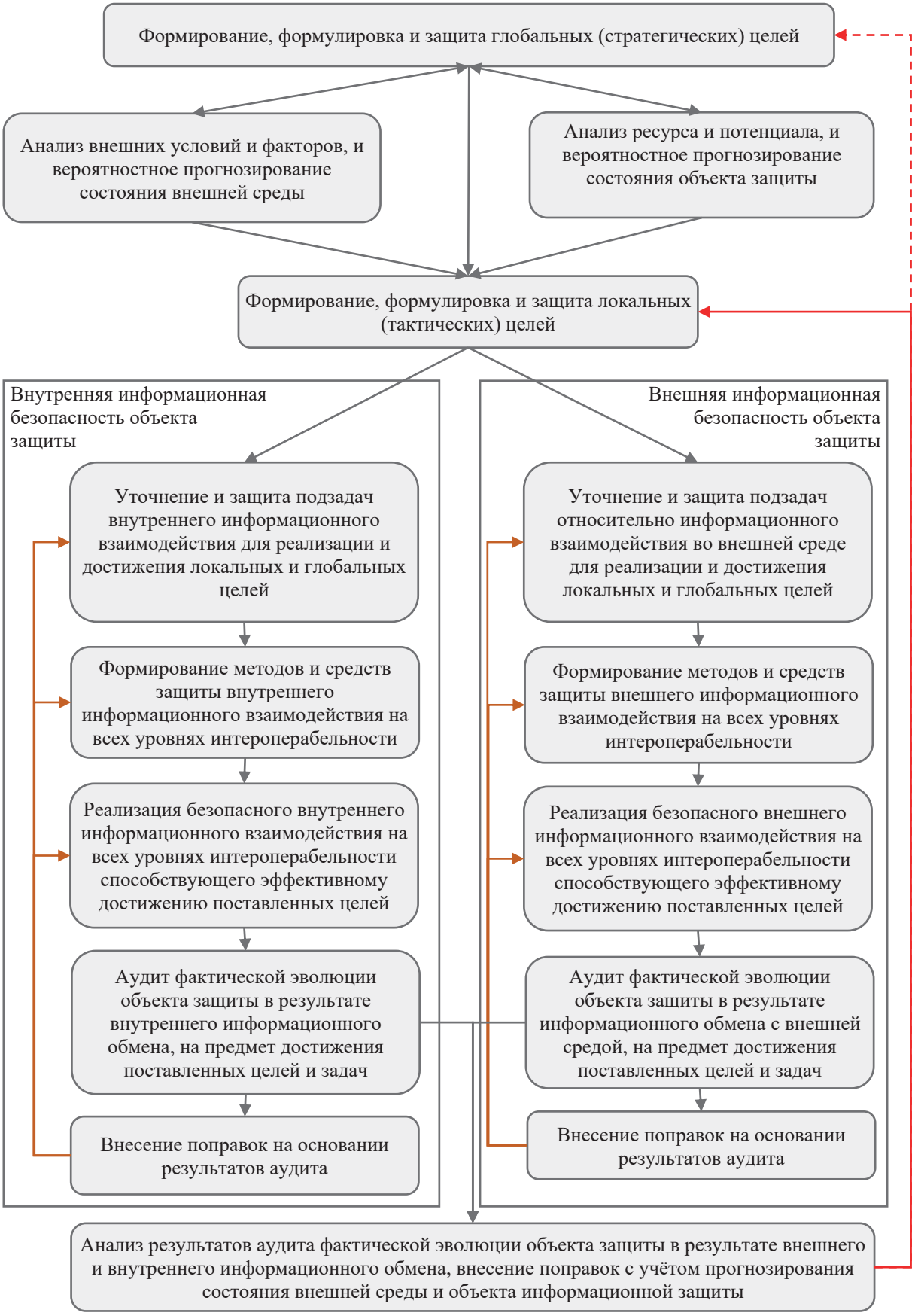

Рис. 3. Графическая модель обеспечения информационной безопасности объекта защиты

необходимая при аудите, формируется из оценок информационного взаимодействия на всех уровнях интероперабельности и способствования информационного взаимодействия достижению поставленной цели объекта защиты.

В соответствии с изложенными принципами сформирована графическая модель обеспечения информационной безопасности объекта защиты (рис. 3). Следует отметить, что данная модель является информационной и потому стрелками обозначены информационные потоки, а блоками ключевые информационные этапы обеспечения безопасности. Изменение стратегических целей объекта защиты может быть связано со значительными изменениями внутреннего состояния объекта защиты и/или внешней среды. Потому стратегические цели вынесены в отдельный блок и в случае устойчивой эволюции объекта защиты достаточно стабильны во времени, потому стрелка, обозначающая внесение поправок, обозначена пунктиром. Локальные (тактические) цели, напротив, изменяются динамично, учитывая состояние объекта защиты и внешней среды. Отдельно реализуются внешняя и внутренняя информационная безопасность объекта защиты. Корректировка подзадач, методов и средств реализации, проводится на основании аудита фактической эволюции объекта защиты в результате информационного взаимодействия внешнего и внутреннего.

Эталонная модель интероперабельности как основа классификации методов и средств информационной безопасности

В таблице 1 дана возможная модель информационной безопасности на основе эталонной модели интероперабельности. По строкам определены уровни интероперабельности (информационного взаимодействия), по столбцам определены уровни обеспечения информационной безопасности. В соответствующих клетках таблицы расположены виды обеспечения информационной безопасности, отвечающие уровню информационного взаимодействия.

Отдельного внимания требует модель аудита информационной безопасности (табл. 2). По строкам, как и в таблице 1, размещены уровни информационного взаимодействия. По столбцам – уровни аудита и оценки рисков информационной безопасности. В клетках таблицы даны соответствующие области аудита и оценки рисков информационной безопасности. Семантический уровень информационной безопасности обеспечивает смысловую защиту информации. Вопрос защиты смыслов требует дополнительного разбора, который в рамках одной публикации сделать затруднительно. В большинстве случаев задача формирования смыслового содержания информации выходит за пределы информационной безопасности, но необходимость сохранения смысла или выявление подмены и/или сокрытия

Таблица 1.

Модель обеспечения информационной безопасности на основе эталонной модели интероперабельности

		Уровни обеспечения информационной безопасности		
		Технический	**Семантический**	**Организационный**
Уровни интероперабельности	**Организационный**	Обеспечение защищённого документооборота	Терминологическое, методическое и методологическое обеспечение информационного взаимодействия объекта защиты	Правовое обеспечение информационной безопасности объекта защиты
	Семантический	Обеспечение конфиденциальности, целостности и доступности информации без учёта её смысловой нагрузки	Обеспечение информационной безопасности объекта защиты за счёт анализа смыслового наполнения при информационном взаимодействии	Формализация целей и задач информационной безопасности, согласно с целями и задачами объекта защиты
	Технический	Обеспечение реализации криптографической, физической и технической защиты	Обеспечение конфиденциальности, целостности и доступности смысловой нагрузки информации	Методическое и методологическое обеспечение технического уровня информационной безопасности

Таблица 2.

Модель угроз, аудита и оценки рисков информационной безопасности на основе эталонной модели интероперабельности

		Уровни обеспечения информационной безопасности		
		Технический	**Семантический**	**Организационный**
Уровни интероперабельности	**Организационный**	Аудит защищённого документооборота	Аудит, ревизия и совершенствование терминологического, методического и методологического обеспечение информационной безопасности	Правовая поддержка, аудита и оценки рисков информационной безопасности
	Семантический	Данные об эффективности методов и средств конфиденциальности, целостности и доступности для построения модели угроз, аудита и оценки рисков информационной безопасности	Комплексный анализ рисков внешнего и внутреннего информационного взаимодействия объекта защиты и прогнозирование на основе моделирования состояния его информационной безопасности. Смысловой аудит управляющей информации с точки зрения обеспечения безопасности объекта информационного взаимодействия.	Аудит и комплексная оценка эффективности результатов применения методов и средств информационной безопасности. Ревизия целей и задач информационной безопасности
	Технический	Аппаратные и аппаратно-программные средства реализации аудита, оценки рисков информационной безопасности и модели угроз	Аудит смысловой нагрузки информации на предмет её конфиденциальности, целостности и доступности	Аудит методического и методологического обеспечения технического уровня информационной безопасности

смысла, а также анализ соответствия смыслового наполнения информации объективному состоянию дел, вполне является задачей информационной безопасности и информационного противоборства.

Как, в целях обеспечения целостности информации производится, например, вычисление *хеш*-функции (от англ. hash function) для некоторого сообщения, и не обязательно эту работу проделывает специалист по информационной безопасности, но специалист владеющей пониманием критериев целостности информации. Так специалист владеющий пониманием целостности смысла информации, может заинтересоваться адекватностью, т.е. соответствию реальному положению дел, относительно, например, принятого сообщения, даже если хеш-функция данного сообщения показывает структурную целостность. Следуя логике защиты интересов стороны информационного взаимодействия, специалист по информационной безопасности должен понимать как те или иные смыслы, наполняющие информацию, повлияют на безопасность объекта защиты в настоящем времени и в будущем, в том числе в отдалённой перспективе, и насколько это влияние способствует эволюции состояния объекта защиты в заданном целевом направлении, т.е. достижению цели. Для такого понимания необходимо располагать целями и задачам объекта защиты интересов информационного взаимодействия на ближайшую и отдалённую перспективу. Например, для защиты государственной информационной безопасности, необходимо располагать целеуказующей идеологией государства, информационная безопасность которого

обеспечивается, с уточняющими комментариями и частными целями.

Как было показано ранее с увеличением значимости и при масштабировании отдельных смыслов формируемых относительно некоторого значительного субъекта хозяйственной деятельности, смыслы трансформируются в идеологию и определяют с одной стороны эволюцию рассматриваемого объекта, а с другой стороны позволяют производить аудит этой эволюции и ключевую управляющую роль в этом процессе имеет смысловой уровень внешнего и внутреннего информационного взаимодействия.

Итак, по мнению авторов, семантический уровень информационной безопасности заключается в защите смыслового наполнения информации. Вопрос защиты и формирования смыслового наполнения информации, является не однозначным и зависит от личностных качеств и идеологических принципов лица или группы лиц осуществляющих смысловое наполнение. Поэтому высокий уровень личной и коллективной ответственности приходится на тех, кто принимает решения о смысловом наполнении и распространении информации, особенно если информация распространяется массово и влияет на мировоззрение значительного числа людей и/или имеет стратегическое значение для развития социальных систем различного масштаба. В этом смысле компетенции специалиста по информационной безопасности имеют характер ценза, способного оценить риски деструктивного информационного влияния. Предмет таких компетенций является не простой задачей, имеет значительное число аспектов, обсуждение которых выходит за рамки данной работы. На сегодняшний день существуют органы, осуществляющие в той или иной степени смысловое регулирование, но делается это зачастую не системно и без опоры на явно обозначенные цели. Но как было показано ранее, это не означает, что целей нет, отсутствие явно сформулированных целей означает, что либо эти цели неизвестны тем, кто реализует частные задачи, либо что их явная формулировка нежелательна по тем или иным причинам.

Обсуждение

Выполненный в работе анализ и синтез моделей информационной безопасности построен на основе исследования с одной стороны современного состояния проблемы и способности к информационному взаимодействию, получившего устоявшееся англоязычное название интероперабельность; с другой стороны современного состояния в области исследований информационной безопасности. Анализ показывает, что интероперабельность, будучи молодым научным направлением за счёт усилий многих учёных по всему миру, выработала устойчивую и обоснованную модель информационного взаимодействия. Сопоставление моделей интероперабельности и информационной безопасности, показывает, что информационная безопасность, не рассматривает в явном виде угрозы и риски при информационном взаимодействии которые связаны с семантическим уровнем информационного взаимодействия, что по мнению авторов является значительной угрозой, особенно для крупных предприятий, организаций и суверенитета Родины. Необходимо отметить, что учёт смысловой составляющей информации в решении задач информационной безопасности не должен обернуться обычной цензурой, запретом, ограничением доступа к информации, подобных явлений и так предостаточно. Напротив, только при максимальной открытости и доступности знаний и объективной информации возможен баланс и безопасность информационной среды. Авторы предлагают за счёт включения в сферу компетенций специалистов по информационной безопасности семантического уровня информационного взаимодействия расширить аналитический инструментарий информационной безопасности, что в свою очередь позволит повысить эффективность информационной безопасности, как в масштабах отдельного предприятия, так и в масштабах страны в целом. Например, анализ и оценка поставленных для объекта защиты целей и оценки результатов её достижения, выявление причин и следствий срыва поставленных целей, выявление возможностей и наличия необходимых ресурсов достижения поставленной цели, критический анализ инструментария и параметров оценивания. Анализ содержательной части имеющихся и вновь принимаемых законов, постановлений на предмет их влияния на национальную безопасность в различных секторах государственной жизни. Разработка инструментария и оценка эффективности информационно-управляющей деятельности организаций и отдельных управленцев. По мнению авторов наиболее опасные информационные угрозы содержаться в смысловом наполнении информации, когда информация не соответствуют действительности, а поставленные цели и задачи не соответствуют фактическому положению дел и объективным возможностям и методам их достижения, и при этом сами сообщения, обеспечивающие необходимый информационный обмен: конфиденциальны, целостны и доступны, но небезопасны в смысле информационно-управляющего эффекта, который эти сообщения осуществляют.

Выводы

На основе анализа научных направлений интероперабельность и информационной безопасность, предлагается дополнить область интересов информационной безопасности семантическим уровнем,

в соответствии с эталонной моделью интероперабельности.

- Выполнен анализ угроз информационной безопасности объекту защиты реализуемых на семантическом уровне информационного взаимодействия.
- В ходе исследований доказана необходимость информационной безопасности на семантическом уровне для обеспечения полноты защиты информационного взаимодействия и удовлетворения интересов объекта информационной защиты.
- Предложена информационная модель разработки и реализации методов информационной безопасности, способствующая достижению целей объекта защиты.
- Предложена модель информационной безопасности на основе эталонной модели интероперабельности.
- Предложена модель аудита и оценки рисков информационной безопасности на основе эталонной модели интероперабельности.

Литература

1. Заседание дискуссионного клуба «Валдай» (дата обращения: 11.11.2024) URL: http://www.kremlin.ru/events/president/news/75521
2. Жаринов И. О. Стек сквозных цифровых технологий как фактор инновационной модернизации оборонно-промышленного комплекса России // Военный академический журнал. 2024. № 3 (43). С. 133–139.
3. Алешковский И. А. Демографический кризис как угроза национальной безопасности России // Век глобализации, 2(10). 2012. 96–114 с.
4. Третьяк О. А., Румянцева М. Н. Сетевые формы межфирменной кооперации: подходы к объяснению феномена // Российский журнал менеджмента. 2003. Т. 1. № 2. С. 25–50.
5. Грановеттер М. Сила слабых связей // Экономическая социология. 2009. Т. 10. № 4. С. 31–50.
6. Введение в теорию управления организационными системами / В. Н. Бурков, Н. А. Коргин, Д. А. Новиков / – М.: Либроком, 2009. 264 с.
7. Поле битвы – киберпространство. Теория, приемы, средства, методы и системы ведения информационной войны / С. Н. Гриняев / – М.: Харвест, 2004. 426 с.
8. О диалекте сдерживания и предотвращения военных конфликтов в информационную эру / И. Н. Дылевский, В. О. Запивахин, С. А. Комов, С. В. Коротков, А. А. Кривченко // Военная мысль. 2016. № 7. С. 3–11.
9. Информационное противоборство и радиоэлектронная борьба в сете-центрических войнах начала XXI века / С. И. Макаренко / – С.-Пб.: Наукоемкие технологии, 2017. 546 с.
10. Макаренко С. И., Олейников А. Я., Черницкая Т. Е. Модели интероперабельности информационных систем // Системы управления, связи и безопасности. 2019. № 4. С. 215–245. DOI: 10.24411/2410-99162019-10408.
11. Гришенцев А. Ю., Коробейников А. Г., Дукельский К. В. Метод численной оценки технической интероперабельности. Кибернетика и программирование. 2017. № 3. С. 23–38.
12. Гришенцев А. Ю., Коробейников А. Г. Средства интероперабельности в распределенных геоинформационных системах. Журнал радиоэлектроники. 2015. № 3. С. 1–18.
13. Интероперабельность человеко-машинных интерфейсов. / С. И. Макаренко / С.-Пб.: Наукоемкие технологии, 2023. 185 с.
14. Вопросы создания единого информационного пространства в системе здравоохранения РАН / Н. Г. Гончаров, Я. И. Гулиев, Ю. В. Гуляев [и др.] // Информационные технологии и вычислительные системы. 2006. № 4. С. 83–95.
15. Информационная безопасность. / С. И. Макаренко / Ставрополь: СФ МГГУ им. М. А. Шолохова, 2009. 372 с.
16. Батоврин В. К., Гуляев Ю. В., Олейников А. Я. Обеспечение интероперабельности – основная тенденция в развитии открытых систем // Информационные технологии и вычислительные системы. 2009. № 5. С. 7.
17. Выдержки из инаугурационной речи президента Дональда Трампа, касающиеся внешней политики. Посольство и консульства США в Российской Федерации. (дата обращения: 03.05.2025) URL: https://ru.usembassy.gov/ru/president-donald-trumps-inaugural-address-ru/.
18. Научная мысль как планетное явление. Избранные труды / В. И. Вернадский / Сост. Г.П. Аксенов. - М.: РОССПЭН, 2010. С.: 580–742.
19. Эпоха потрясений / А. Гринспен / – М.: Альпина Бизнес Букс, 2007. 90 с.
20. Кризис. Как это делается / Н. Стариков / – С.-Пб.: Питер, 2010. 304 с.
21. Цель жизни. Записки авиаконструктора. 5-е изд., переработ. и доп. / А. С. Яковлев / – М.: Политиздат, 1987. 511 с.
22. Моя жизнь, мои достижения / Г. Форд / Пер. под ред. В. А. Зоргенфрея; предисл. Н. С. Лаврова. – Л.: Время, 1924. 326 с.
23. Выдающийся русский ученый-электрик академик Владимир Федорович Миткевич / М. А. Шателен, Л. Р. Нейман, И. А. Зайцев [и др.] // Электричество. 2005. № 1. С. 89–91.
24. Коровкин Н. В. Академик Владимир Федорович Миткевич (к 150-летию со дня рождения). Электричество. 2022. № 8. С. 65–69. DOI 10.24160/0013-5380-2022-8-65-69.
25. Заколдаев Д. А., Гришенцев А. Ю. Методология моделирования и обеспечения информационной безопасности при управлении ресурсами // Вестник компьютерных и информационных технологий. 2021. Т. 18. № 4 (202). С. 45–52. DOI 10.14489/vkit.2021.04.pp. 045–052
26. Заколдаев Д. А., Гришенцев А. Ю. Формальная модель обеспечения информационной безопасности при управлении ресурсами на производствах // Системы управления, связи и безопасности. 2021. № 1. С. 33–61. DOI 10.24411/2410-9916-2021-10102.

INTEROPERABILITY AS A BASIS FOR SYSTEMATIZATION OF INFORMATION SECURITY METHODS AND MEANS

Grishentsev A. Yu.[9], Korovkin N. V.[10], Korobeynikov A. G.[11]

Keywords: *information protection, information interaction, open systems, models, standards.*

Purpose of the study: *development of the theoretical foundations of information security through sound systematization, methods and means of information security based on the concept of interoperability.*

Methods of research: *analysis of information interaction and threats in information interaction based on a standardized reference model of interoperability and synthesis of a systematic structured model of information security methods and tools in the context of the concept of interoperability.*

Result's: *based on the analysis of scientific areas of interoperability and information security, it is proposed to supplement the field of interests of information security with a semantic level, in accordance with the reference model of interoperability. The analysis of information security threats to the object of protection implemented at the semantic level of information interaction has been performed. In the course of research, the need for information security at the semantic level has been proved to ensure the completeness of information interaction protection and to satisfy the interests of the information protection object. An information model for the development and implementation of information security methods is proposed to help achieve the objectives of the object of protection. A model of information security based on a reference model of interoperability is proposed. A model of information security audit and risk assessment based on a reference model of interoperability is proposed.*

Scientific novelty: *It consists in a new approach to systematization of methods, means and increasing the sphere of interests of information security based on modern scientific ideas about the levels of information interaction in accordance with the concept of interoperability.*

References

1. Zasedanie diskussionnogo kluba «Valdaj» (2024, November 07). URL: http://www.kremlin.ru/events/president/news/75521.
2. Zharinov, I. O. (2024). Stek Skvoznyx Cifrovyx Texnologij Kak Faktor Innovacionnoj Modernizacii Oboronno-Promyshlennogo Kompleksa Rossii. Voennyj Akademicheskij Zhurnal, 2(10), 133–139.
3. Aleshkovskij, I. A. (2012). Demograficheskij Krizis Kak Ugroza Nacional'noj Bezopasnosti Rossii. Vek Globalizacii, 2(10), 96–114. https://www.socionauki.ru/journal/articles/147957/.
4. Tret'yak, O. A., & Rumyanceva, M. N. (2003). Setevye Formy Mezhfirmennoj Kooperacii: Podxody k Ob''yasneniyu Fenomena. Rossijskij Zhurnal Menedzhmenta, 2, 25–50. https://rjm.spbu.ru/article/view/812/707.
5. Granovetter, M. (2003). Sila Slabyx Svyazej (Z. V. Kotel'nikova, Trans.). Ekonomicheskaya Sociologiya, 10(4), 31–50. https://ecsoc.hse.ru/2009-10-4/26591138.html.
6. Burkov V. N., Korgin N. A., Novikov D. A. (2009). Vvedenie v teoriyu upravleniya organizacionnymi sistemami. Librokom. 264 p.
7. Grinyaev S. N. (2004). Pole bitvy – kiberprostranstvo. Teoriya, priemy, sredstva, metody i sistemy vedeniya informacionnoj vojny. Harvest. 426 p.
8. Dylevskij I. N., Zapivaxin V. O., Komov S. A., Korotkov S. V. & Krivchenko A. A. (2016) O dialekte sderzhivaniya i predotvrashheniya voennyx konfliktov v informacionnuyu eru. Voennaya mysl'. 7, 3–11.
9. Makarenko S. I. (2017). Informacionnoe protivoborstvo i radioelektronnaya bor'ba v sete-centricheskix vojnax nachala XXI veka. Naukoemkie texnologii. 546 p.
10. Makarenko S. I., Olejnikov A. Ya., Chernickaya T. E. (2019). Modeli interoperabel'nosti informacionnyx system. Sistemy upravleniya, svyazi i bezopasnosti. 4, 215–245. DOI: 10.24411/2410-99162019-10408.
11. Grishencev A. Yu., Korobejnikov A. G., Dukel'skij K. V. (2017). Metod chislennoj ocenki texnicheskoj interoperabel'nosti. Kibernetika i programmirovanie. 3, 23–38.
12. Grishencev A. Yu., Korobejnikov A. G. (2015). Sredstva interoperabel'nosti v raspredelennyx geoinformacionnyx sistemax. Zhurnal radioelektroniki. 3, 1–18.
13. Makarenko S. I. (2023). Interoperabel'nost' cheloveko-mashinnyx interfejsov. Naukoemkie texnologii. 185 p.
14. Goncharov N. G., Guliev Y. I., Gulyaev Y. V., Kavinskaya A. A., Olejnikov A. Y., & Xatkevich M. I. (2006). Voprosy Sozdaniya Edinogo Informacionnogo Prostranstva v Sisteme Zdravooxraneniya RAN. Informacionnye Texnologii i Vychislitel'nye Sistemy, 4, 83–95. https://jitcs.frccsc.ru/arhiv/2006/release_4/voprosy_sozdaniya_edinogo_informatsionnogo_prostranstva_v_sisteme_zdravoohraneniya_ran.html.

9 Alexey Yu. Grishentsev, Dr.Sc. of Technical Sciences, Associate Professor, Corresponding Member of the Academy of Electrotechnical Sciences of the Russian Federation, Associate Professor of the Federal State Autonomous Educational Institution of Higher Education ITMO National Research University. St. Petersburg, Russia. E-mail:AGrishentsev@yandex.ru

10 Nikolay V. Korovkin, Dr.Sc. of Technical Sciences, Professor, Full Member of the Academy of Electrotechnical Sciences of the Russian Federation, Professor of the Federal State Autonomous Educational Institution of Higher Education Peter the Great St. Petersburg Polytechnic University. St. Petersburg, Russia. E-mail: Nikolay.Korovkin@gmail.com

11 Anatoly G. Korobeynikov, Dr.Sc. of Technical Sciences, Professor, Deputy Director for Science of the St. Petersburg Branch of the Pushkov Institute of Terrestrial Magnetism, Ionosphere and Radio Wave Propagation of the Russian Academy of Sciences, Professor of the Federal State Autonomous Educational Institution of Higher Education ITMO National Research University. St. Petersburg, Russia. E-mail: Korobeynikov_A_G@mail.ru

15. Makarenko S. I. Informacionnaya bezopasnost'. (2009). SF MGGU im. M. A. Sholoxova. 372 p.
16. Batovrin V. K., Gulyaev Y. V., & Olejnikov A. Y. (2006). Obespechenie Interoperabel'nosti – Osnovnaya Tendenciya v Razvitii Otkrytyx Sistem. Informacionnye Texnologii I Vychislitel'nye Sistemy, 2009. № 5. Pp. 7. http://www.jitcs.ru/index.php?option=com_content&view=article&id=310.
17. Trump, D. (2025, January 22). President Donald Trump's Inaugural Address. Ru.Usembassy.Gov. https://ru.usembassy.gov/president-donald-trumps-inaugural-address/.
18. Vernadskij V. I. (2010). Nauchnaya Mysl' Kak Planetnoe Yavlenie. Izbrannye Trudy (Aksenov G. P.). ROSSPEN. 742 p.
19. Grinspen, A. (2007). Epoxa Potryasenij. Al'pina Biznes Buks. 90 p.
20. Starikov N. (2010). Krizis. Kak eto delaetsya. Piter. 304 p.
21. Yakovlev A. S. (1987). Cel' Zhizni. Zapiski Aviakonstruktora (5th ed.). Politizdat. 511 p.
22. Ford, G. (1922). My Life and Work. Stone Hedge. 304 p.
23. Shatelen, M. A., Nejman, L. R., & Zajcev, I. A. (2005). Vydayushhijsya Russkij Uchenyj-Elektrik Akademik Vladimir Fedorovich Mitkevich. Elektrichestvo, 1, 89–91.
24. Korovkin, N. V. (2022). Akademik Vladimir Fedorovich Mitkevich (k 150-letiyu so dnya rozhdeniya). Elektrichestvo, 2, 65–69. DOI 10.24160/0013-5380-2022-8-65-69.
25. Zakoldaev, D. A., Grishentsev, A. Yu. (2021). Methodology for modeling and ensuring information security in resource management. Herald of computer and information technologies, 4(202), 45–52. DOI: 10.14489/vkit.2021.04.pp.045-052.