

УДК 004.056

**ОРГАНИЗАЦИОННЫЕ ПОДХОДЫ К МОДЕРНИЗАЦИИ СИСТЕМЫ
ОБЕСПЕЧЕНИЯ ИНФОРМАЦИОННОЙ БЕЗОПАСНОСТИ В
ОРГАНАХ ГОСУДАРСТВЕННОЙ ВЛАСТИ ДОНЕЦКОЙ НАРОДНОЙ
РЕСПУБЛИКИ**

Г.С. Джура, соискатель

ГОУ ВПО «Донецкий национальный
технический университет»,
г. Донецк, ДНР,
e-mail: dzhura_egor95@mail.ru

**ORGANIZATIONAL AND ECONOMIC APPROACHES TO THE
MODERNIZATION OF THE INFORMATION SECURITY SYSTEM IN THE
STATE AUTHORITIES OF THE DONETSK PEOPLE'S REPUBLIC**

G.S. Dzhura, applicant

SEI HPE «Donetsk National Technical
University», Donetsk, DPR,
e-mail: dzhura_egor95@mail.ru

Реферат

Цель статьи состоит в совершенствовании организационных подходов к модернизации системы обеспечения информационной безопасности в органах государственной власти Донецкой Народной Республики.

Методика. В процессе исследования использованы теоретические и эмпирические методы, а именно: анализ, синтез, сравнение, обобщение и описание.

Результаты. В статье на основе анализа современных подходов обоснована целесообразность модернизации систем обеспечения информационной безопасности (далее – СОИБ) в органах государственной власти (далее – ОГВ) Донецкой Народной Республики (далее – ДНР), опираясь на российский опыт. Определены ключевые цели задачи и ожидаемых результатов от внедрения предлагаемых положений.

Научная новизна. Обоснована необходимость создания Единого координационного ситуационного центра в сфере обеспечения информационной безопасности ОГВ, что позволит оптимизировать процессы взаимодействия органов-регуляторов в сфере информационной безопасности, Правительства ДНР и других органов, а также повысить эффективность, зрелость и оперативность принятия управленческих решений на общегосударственном уровне.

Практическая значимость. Модернизация СОИБ в ОГВ с учетом их особенностей в соответствии с целью и сферой применения повышает прозрачность и контролируемость процессов информационной безопасности (далее – ИБ) и способствует оптимизации общего состояния ИБ ДНР.

Ключевые слова: *информационная безопасность, организационные подходы, органы государственной власти, система обеспечения информационной безопасности.*

Постановка проблемы и ее связь с важными научными и практическими задачами. Сегодня современное цифровое общество находится на беспрецедентном уровне развития и проникновения в жизнь человека технологической составляющей. С учетом вышесказанного сложно отрицать, что общегосударственная безопасность может быть обеспечена без информационной составляющей. В связи с этим любое современное государство имеет шансы на устойчивое развитие только в условиях учета данных тезисов. «Кто не идет вперед, тот идет назад: стоячего положения нет» Белинский В.Г. [1] Данное развитие, в рамках противодействия хаосу в цифровой среде, с учетом все нарастающего спектра и глубины рисков информационной безопасности может быть обеспечено исключительно на высшем государственном уровне, ключевыми элементами которого являются органы государственной власти (далее – ОГВ).

Стоит отметить, что от своевременности осознания указанных выше положений зависит качество и скорость развития многих сфер и отраслей в рамках развития информационно-технологической сферы, в общем, и неотъемлемо сопровождающей ее сферы информационной безопасности (далее – ИБ), в частности.

Анализ последних исследований и публикаций. Существенный вклад в развитие подходов к модернизации общегосударственной системы обеспечения информационной безопасности (далее – СОИБ) как научного направления внесли А.Н. Кубанков, Н.Н. Куняев [2], Е. В. Вострецова [3]. Среди современных ученых, занимающихся изучением проблем модернизации систем обеспечения информационной безопасности ОГВ, заслуживают внимания работы таких авторов, как: Ю.В. Вовенда [4], Ю.Н. Загинайлов [5], Л.В. Лось [6], А.Н. Кухарский [7] и др. Благодаря многочисленным исследованиям перечисленных авторов становится возможным обоснованное применение организационно-экономических подходов к модернизации СОИБ в ОГВ ДНР.

Цель статьи – совершенствование организационных подходов к модернизации СОИБ в ОГВ ДНР с учетом их особенностей и сферы применения.

Изложение основного материала исследования. В то время как в мире полным ходом создаются государственные программы по обеспечению ИБ [8], формируются центры и институты, целью которых является совершенствование подходов к обеспечению ИБ, принимаются общегосударственные концепции и нормы, которые закрепляются на конституционном уровне, в информационно-технологическом пространстве ДНР накапливается масса требующих всесторонней оптимизации направлений.

Количество информационных ресурсов в Республике постоянно растет наряду с важностью и чувствительностью данных, циркулирующих в них. Компьютерные атаки активно проводятся на информационные ресурсы ОГВ. Производится это как в рамках геополитических инициатив, так и с множеством других разнородных целей.

Нет возможности привести статистические данные с конкретизацией ОГВ ДНР и масштаба произошедших с их информационными ресурсами инцидентов, как по причине отсутствия ведения на территории Республики таковой статистики, так и в рамках отсутствия возможности запросить данные у уполномоченных структур на работу в данной сфере. Однако, тот факт, что как количество регистрируемых инцидентов, так и масштаб их последствий, в Республике в том числе с учетом трансграничных и геополитических особенностей является внушительным и требует разноаспектной оптимизации не поддаётся сомнению.

С учетом постоянно совершенствующихся методов и способов компрометации данных, разрозненные децентрализованные методы к обеспечению ИБ в ОГВ, делают невозможным формирование полноценного системного подхода. Организационная структура ДНР в сфере ИБ схожа со структурой Российской Федерации (далее – РФ), т.к. базируется на ее нормативно-правовой базе, однако, такие аспекты, как: неразработанные подзаконные нормативно-правовые акты, недостаточно определенные полномочия ОГВ, указанные в законах и отсутствие стратегических подходов в сфере говорят о явной необходимости всестороннего пересмотра существующих подходов. Поэтому с целью оптимизации общегосударственных подходов в указанной сфере важным является проведение анализа опыта РФ в данной сфере.

Стоит отметить, что общегосударственные подходы к ИБ РФ строятся на основе разграничения полномочий органов законодательной, исполнительной и судебной власти федерального, субъектного и ведомственного уровня, а также служб предприятий и организаций. С целью анализа организационной структуры регуляторов РФ в сфере ИБ важным представляется рассмотрение представленной на рис. 1 иерархии государственных структур.

Правительство РФ координирует деятельность федеральных органов исполнительной власти (далее – ФОИВ) по реализации первоочередных задач в сфере ИБ, регулирует и совершенствует деятельность государственной СОИБ, формирует в установленном порядке статьи федерального бюджета в целях обеспечения ИБ и реализации федеральных целевых программ в указанной области, а также утверждает федеральные целевые программы по обеспечению безопасности информационного общества.

Ключевыми органами, осуществляющими регуляторное, контрольное и надзорное обеспечение регулирования сферы ИБ в РФ являются Федеральная служба безопасности (далее – ФСБ) и Федеральная служба технического и экспортного контроля (далее – ФСТЭК) со своими управлениями по территориальным округам.

ФСТЭК РФ организует деятельность государственной СОИБ, осуществляет межотраслевую координацию и функциональное регулирование деятельности в области ИБ, а также государственный контроль в этой области.

Минобороны РФ, ФСБ, Министерство внутренних дел РФ (МВД), Служба внешней разведки РФ (СВР), Федеральная служба охраны РФ (ФСО) Центральный банк РФ, координируют, организуют, обеспечивают и контролируют в пределах своей компетенции деятельность в области ИБ в соответствующих сферах и подведомственных организациях.

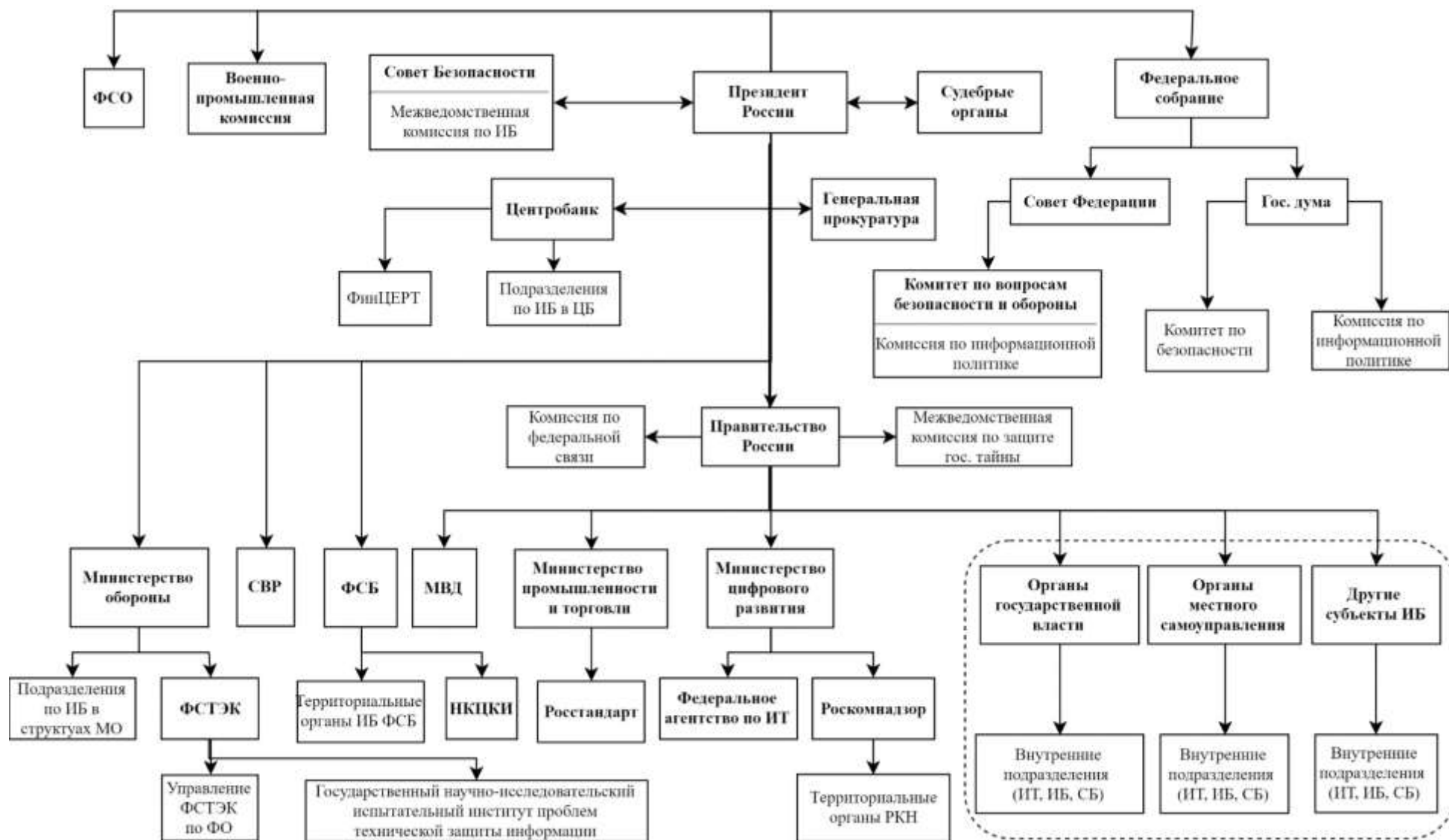


Рисунок 1 – Организационная структура ключевых субъектов регулирования ИБ в РФ

Органы исполнительной власти субъектов и органы местного самоуправления в РФ, являясь следующим уровнем субъектов регулирования в сфере ИБ, взаимодействуя с федеральными органами исполнительной власти по вопросам исполнения законодательства, решений Президента и Правительства и реализации федеральных программ в указанной сфере, совместно осуществляют мероприятия по привлечению граждан и организаций, а также вносят в федеральные органы исполнительной власти предложения по совершенствованию общегосударственных подходов к ИБ РФ.

На уровне областей разрабатываются и реализуется соответствующая законодательная база. Правительство областей разрабатывает и принимает муниципальные программы в рассматриваемой сфере. Органы местного самоуправления отвечают за соблюдение законодательства РФ в области обеспечения ИБ. Органы судебной власти и прокуратуры субъектов РФ осуществляют правосудие по делам о преступлениях, связанных с информационной сферой. В структуре органов исполнительной власти субъектов РФ созданы специальные службы и комиссии, деятельность которых направлена на организацию процессов информатизации, а также разработку нормативно-правовых актов регионального уровня.

Кроме того, в состав важнейших субъектов в сфере ИБ РФ входит совокупность систем и организаций, обеспечивающих ее функционирование, в том числе:

- система научного и нормативно-методического обеспечения работ в сфере ИБ;
- система лицензирования деятельности в области ИБ;
- организации, осуществляющие разработку и производство средств ИБ, а также оказывающие услуги в области ИБ;
- система обязательного подтверждения соответствия средств ИБ, процессов их производства, хранения, перевозки, реализации и утилизации установленным требованиям;
- единая информационно-аналитическая система обеспечения деятельности государственной системы ИБ;
- система подготовки, переподготовки и повышения квалификации специалистов в области ИБ.

Ориентируясь на опыт РФ, стоит отметить, что существующие в Республике проблемы могут быть решены с помощью оптимизации организационной и технической структуры ОГВ ДНР, в частности, создания Единого государственного координационного центра органов государственной власти (далее – ЕГКЦ), для оптимизации процесса развития которого необходимо определить этапы создания, поддержки и развития органа (табл. 1).

Таблица 1 – Этапы создания ЕГКЦ

Этап	Содержание
Разработка концепции построения центра ЕГКЦ	Формирование стратегического плана, содержащего цели, задачи и поэтапный план развития
Разработка операционной и организационной модели ЕГКЦ	Формирование операционной и организационной модели (в т.ч. организационно-штатной структуры) с учетом требований, заложенных в законодательстве ДНР
Разработка архитектуры центра ЕГКЦ	1. Формирование, согласование и утверждение архитектуры ЕГКЦ (информационной инфраструктуры, инструментов, ресурсов для обеспечения функциональной деятельности и др. 2. Разработка процессов центра ЕГКЦ с привязкой к бизнес-процессам и информационной инфраструктуре
Определение списка предоставляемых сервисов	На начальном этапе целесообразно оптимизируя штат ЕГКЦ предоставлять только некоторые из основных сервисов. После пилотного запуска список может быть расширен
Составление Бизнес-Плана	1. Финансовая Модель (электронные сервисы ОГВ – в т.ч. государственные услуги должны работать круглосуточно, что говорит о необходимости предоставления в рабочие часы ЕГКЦ услуг в полном объеме, а в нерабочее время услуги будут предоставляться по требованию. 2. Модель Доходов (во время пилотного этапа ЕГКЦ может финансироваться из Республиканского бюджета. С пилотного этапа по оценочный будет рассмотрен вопрос привлечения дополнительного финансирования, включая возможность продажи услуг внешним потребителям). 3. Организационная модель, штат сотрудников (определение организационной модели, штата сотрудников и уровня их подготовки). 4. Создание бизнес-плана (подготовка экономического обоснования и плана проекта, а также расчет затрат на наладочные работы и расчет эксплуатационных расходов)
Формализация процессов, процедур, систематизация функциональной деятельности	1. Определение последовательности технологических процессов, порядка действий и технических процедур. 2. Разработка необходимой нормативной документации для создания ЕГКЦ
Разработка ключевых показателей эффективности	Разработка и согласование с Правительством показателей (факторов) для оценки эффективности процессов ЕГКЦ
Внедрение технических средств ЕГКЦ	Формирование информационной инфраструктуры и ресурсов, обеспечивающих процессы ЕГКЦ
Внедрение разработанных процессов	Начало функционирования ЕГКЦ. Реализация функций и полномочий организации
Контроль эффективности внедренных процессов	1. Разработка показателей оценки эффективности. 2. Формирование отчетов в соответствии с разработанными показателями
Разработка системы аналогичной мониторинга ОГВ в сфере ИБ	Разработка автоматизированной информационной системы обнаружения, предупреждения и ликвидации последствий компьютерных атак с целью всесторонней оптимизации процессов координации ОГВ в рамках реагирования на инциденты и др. процессов совершенствования СОИБ в ОГВ
Подготовка, переподготовка кадров	Совершенствование знаний и подготовки ответственных сотрудников ЕГКЦ и ОГВ

Следует отметить, что указанный подход с ориентиром на опыт РФ поможет заложить прочный фундамент в совершенствование общего уровня ИБ в ДНР и будет способствовать решению следующих ключевых задач:

1. В части организационного обеспечения ИБ:
 - координация ОГВ в сфере обеспечения ИБ;

- оценка и поддержание уровня обеспечения ИБ в ОГВ;
- упрощение потенциального подключения к государственной СОИБ РФ;

- систематизация государственных подходов к обеспечению ИБ.

2. В части нормативного обеспечения ИБ:

- помощь гражданам в обеспечения ИБ;
- разработка и совершенствование законодательства в сфере ИБ;
- создание систем лицензирования и сертификации систем и средств обеспечения ИБ;

3. В части организационно-технической защиты информации:

- выявление признаков, предупреждение и ликвидация последствий компьютерных атак, определение их источников, методов, способов и средств осуществления и направленности, а также разработка методов и средств обнаружения;

- формирование и поддержание в актуальном состоянии детализированной информации об информационных ресурсах ДНР;

- прогнозирование ситуации в области обеспечения ИБ ДНР, включая выявленные и прогнозируемые угрозы и их оценку;

- организация и осуществление взаимодействия с правоохранительными и другими ОГВ, владельцами информационных ресурсов ДНР, операторами связи, интернет-провайдерами и иными заинтересованными организациями на национальном и международном уровнях в области обнаружения компьютерных атак и установления их источников, включая обмен информацией о выявленных компьютерных атаках и вызванных ими компьютерных инцидентах, а также обмен опытом в сфере выявления и устранения уязвимостей программного обеспечения и оборудования и реагирования на компьютерные инциденты;

- организация и проведение научных исследований в сфере разработки и применения средств и методов обнаружения, предупреждения и ликвидации последствий компьютерных атак;

- осуществление мероприятий по обеспечению подготовки и повышению квалификации кадров в сфере обеспечения ИБ;

- сбор и анализ информации о компьютерных атаках и вызванных ими компьютерных инцидентах в отношении информационных ресурсов ДНР, а также о компьютерных инцидентах в информационных системах и информационно-телекоммуникационных сетях других стран, с которыми взаимодействуют владельцы информационных ресурсов ДНР;

- осуществление мероприятий по оперативному реагированию на компьютерные атаки и вызванные ими компьютерные инциденты, а также по ликвидации последствий данных компьютерных инцидентов в информационных ресурсах ДНР;

- мониторинг степени защищенности государственных информационных ресурсов и информационно-телекоммуникационных сетей на всех этапах создания, функционирования и модернизации информационных ресурсов ДНР, а также разработка методических рекомендаций по организации защиты информационных ресурсов ДНР от компьютерных атак;

- совершенствование оперативно-тактического взаимодействия сил и средств обнаружения, предупреждения и ликвидации последствий компьютерных атак.

Выводы и перспективы дальнейших исследований. Стоит отметить, что общегосударственные подходы к ИБ в ДНР также, как и Республика в целом, находится на начальной стадии своего становления и подходы к созданию, поддержанию и развитию системы, по мнению автора, нуждаются в оптимизации, которую сложно реализовать в современных экономических и политических условиях становления Республики. В связи с этим, совершенствование системных подходов к обеспечению ИБ ОГВ нуждаются во всесторонней непрерывной комплексной поддержке, которая не может быть обеспечена без организационной и регуляторной составляющей.

Конкретным способом оптимизации существующих вопросов, по мнению автора, является создание единого государственного координационного центра по обеспечению информационной безопасности ОГВ. Преимуществами предложенного централизованного подхода являются:

- минимизация дублирования работ по созданию СОИБ в ОГВ;
- четкость и прозрачность определения необходимых функций и ответственности в сфере обеспечения ИБ;
- повышение оперативности принятия решений в сфере обеспечения ИБ;
- формирование единых стандартов, форматов представления данных и результатов их обработки;
- повышение эффективности системы контроля работы подразделений ИБ ОГВ со стороны руководства ОГВ и Правительства ДНР;
- оперативное формирование статистических отчетов по инцидентам ИБ;
- создание системы мониторинга текущего состояния СОИБ в ОГВ;

– совершенствование инструментов для быстрого выявления и купирования инцидентов ИБ в ОГВ.

Список литературы

1. Цитаты известных личностей [Электронный ресурс]. – Режим доступа: <https://ru.citaty.net/tsitaty/613987-vissarion-grigorevich-belinskii-kto-ne-idiot-vperiod-tot-idiot-nazad-stoiachego-polozh/> (дата обращения: 12.02.2021).

2. Кубанков А. Н. Система обеспечения информационной безопасности Российской Федерации: организационно-правовой аспект: учебное пособие / А. Н. Кубанков, Н. Н. Куняев – Москва: Всероссийский государственный университет юстиции (РПА Минюста России), 2014. – 78 с.

3. Вострецова Е. В. Основы информационной безопасности: учебное пособие / Е. В. Вострецов. – Екатеринбург: Министерство образования и науки Российской Федерации, Федеральное Уральский федеральный университет имени первого Президента России Б.Н. Ельцина, 2019 – 208

4. Вовенда Ю. В. Особенности политики обеспечения информационной безопасности в исполнительных органах государственной власти (на примере Северо-Западного федерального округа): дис. ... канд. полит. наук: 23.00.02 – «Политические институты, процессы и технологии» / Вовенда Юлия Владимировна; ФГБОУ ВПО «Санкт-Петербургский государственный университет». – Санкт-Петербург, 2019. – 213 с.

5. Загинайлов Ю. Н. Определение состава и структуры системы обеспечения информационной безопасности России [Электронный ресурс] / Ю. Н. Загинайлов. – Режим доступа: <http://edu.secna.ru/media/f/zag2-02.pdf> (дата обращения: 12.02.2021).

6. Лось Л. В. Информационная безопасность в системе национальной безопасности Российской Федерации / Л. В. Лось // Вопросы российского и международного права. – 2019. – Т.9. №3А. – С. 159-170.

7. Кухарский А.Н. Информационная безопасность политического процесса как элемент государственного и муниципального управления России: дис. ... канд. полит. наук: 23.00.02 – «Политические институты, процессы и технологии» / Кухарский Артем Николаевич; ФГБОУ ВО «Забайкальский государственный университет». – Чита, 2019 – 199 с.

8. План мероприятий по направлению «Информационная безопасность» программы «Цифровая экономика Российской Федерации» [Электронный ресурс]. – Режим доступа: <http://static.government.ru/media/files/AEO92iUpNPX7Aaonq34q6BxpАНСY2umQ.pdf>