О РЕАЛИЗАЦИИ НОВЫХ ТРЕБОВАНИЙ ЗАКОНОДАТЕЛЬСТВА РОССИЙСКОЙ ФЕДЕРАЦИИ О ЗАЩИТЕ ИНФОРМАЦИИ В ГОСУДАРСТВЕННЫХ ИНФОРМАЦИОННЫХ СИСТЕМАХ

Волостных В. А.[1], Задбоев В. А.[2], Шевченко А. А.[3]

DOI:10.21681/3034-4050-2026-4-84-92

Ключевые слова: *информационные системы, криптография, угрозы безопасности, информационная безопасность, правовые документы.*

Аннотация

Цель работы: *проанализировать действующие изменения требований к безопасности государственных информационных систем и разработать подходы к их внедрению в современных условиях.*

Результаты исследования: *рассмотрены изменения требований российских нормативных документов в области информационной безопасности в государственных информационных системах, не затрагивая информацию по государственной тайне.*

На основе анализа современного применения практического опыта в области защиты информации в организациях, предложены рекомендации по обновлению систем защиты в соответствии с нововведениями. Показаны основные проблемы развития систем безопасности крупных информационных систем и пути их решения, определены существенные изменения в законодательстве о защите информации, разработаны предложения по рекомендации обновления систем защиты в соответствии с нововведениями, для обеспечения безопасности информации, обрабатываемой в информационно-телекоммуникационных системах предприятий, организаций, воинских частей и учреждений.

Практическая полезность: *заключается в том, что в рамках единого исследования проводится системное документальное сравнение ряда нормативных правовых документов и выработаны рациональные подходы к реализации требований в современных условиях, которые могут быть применены при обеспечении безопасности информации в информационных системах предприятий, организаций, воинских частей и учреждений.*

Введение и постановка задачи

В современных условиях информационные системы (ИС) Российской Федерации подвергаются множеству угроз, среди которых компьютерные атаки, направленные на государственные информационные системы (ГИС), занимают одно из ведущих мест. В последние годы в связи с известными событиями наблюдается значительный рост компьютерных атак, направленных на нарушение безопасности информационных ресурсов (ИР) и на нарушение работоспособности ИС. Такие атаки могут полностью остановить работу предприятий, организаций и воинских частей, нарушить или серьёзно затруднить работу их информационных систем и тем самым нанести значительный ущерб государству. В условиях цифровой трансформации и растущей зависимости управленческих решений от безопасности информационных ресурсов и качества функционирования ИС, их защищенность приобретает важнейшее значение. Вопросы защиты информационных ресурсов рассматривались в ряде работ [1–5], но рассмотренные в данных работах материалы, во-первых, несколько устарели и кроме того, рассматриваемые подходы к защите информационных ресурсов касались в основном негосударственных ИС, и из этого следует необходимость данного исследования.

В России вопросам информационной безопасности (ИБ) уделяется серьёзное внимание [6–8]. В 2000 году была принята «Доктрина информационной безопасности Российской Федерации», обновленная в 2016 года. В 2021 г. Указом Президента РФ № 400 была утверждена новая Стратегия национальной безопасности Российской Федерации, которая вышла в свет несколько раньше установленного срока. Обновление подобных «стратегических» документов вызвано, во-первых, появлением новых угроз в сфере информационной безопасности, а во-вторых, изменением технологий обработки информации. В последние пять лет во исполнение Стратегии национальной безопасности вышел ряд новых документов, определяющих требования к защищенности государственных информационных ресурсов. В целях выработки подходов к реализации данных требований

1 ***Волостных Виктор Анатольевич***, кандидат военных наук, доцент, научный сотрудник Военной академии связи, г. Санкт-Петербург, Россия. E-mail: ra1alo@mail.ru

2 ***Задбоев Вадим Александрович***, младший научный сотрудник Военной академии связи, г. Санкт-Петербург, Россия. E-mail: zadboev89@mail.ru

3 ***Шевченко Александр Александрович***, кандидат технических наук, доцент, старший научный сотрудник Военной академии связи, г. Санкт-Петербург, Россия. E-mail: alex_pavel1991@mail.ru

необходимо провести их анализ и определить перечень основных первоочередных мероприятий по обеспечению защиты информационных ресурсов, обрабатываемых в ГИС.

Постановка задачи в данной работе заключается в анализе новых требований законодательства Российской Федерации, их существенных особенностей и в разработке рациональных мероприятий по их реализации в современных условиях.

Под современными условиями функционирования ГИС в работе понимаются:

- высокая интенсивность сложных компьютерных атак [9–10];
- сложность финансирования мероприятий по обеспечению информационной безопасности; отсутствие требуемого количества подготовленного персонала подразделений технической защиты (информационной безопасности);
- отсутствие четкой методологии защиты государственных информационных ресурсов.

В соответствии с законодательством в работе используется следующая терминология:

1. Информационная система – совокупность данных в базах и средств, которые обеспечивают их обработку: программ, технологий и оборудования.
2. ГИС – федеральные и региональные ИС, созданные на основании законов РФ, законов субъектов или решений государственных органов. Данные, которые хранятся в ГИС, а также другие документы и сведения госорганов относятся к государственным информационным ресурсам.

Задача исследования – определить основные первоочередные меры путем анализа действующего законодательства и выявить необходимые для выполнения этих требований и приведения систем защиты ГИС в соответствие с действующими нормами.

Решение поставленной задачи

При решении поставленной задачи был составлен перечень основных нормативных правовых документов по защите информационных ресурсов в ГИС, вступивших в силу в последние пять лет и выделены основные новые требования к защите информации, которые в явном виде законодательством не были установлены. В данный перечень (табл. 1) не входят документы, определяющие порядок защиты государственной тайны и объектов критической информационной инфраструктуры.

Анализ нормативных правовых документов, определяющих требования по защите государственных информационных ресурсов, приведен ниже:

1. Основополагающим документом в сфере защиты информации является **Федеральный закон от 27 июля 2006 г. № 149-ФЗ «Об информации, информационных технологиях и о защите информации»**, который систематически дополняется и уточняется.

В обновленной редакции закона определено, что ГИС создаются для выполнения задач госорганов и обмена данными между ними, а также для других целей, установленных федеральными законами.

Такие системы разрабатываются, обновляются и используются с учётом требований законодательства Российской Федерации.

Правительство Российской Федерации устанавливает правила создания, развития, ввода в работу, эксплуатации и вывода из эксплуатации ГИС, а также порядок хранения данных в их базах. В этих правилах прописаны этапы работ и сроки их выполнения.

Так же в обновленной редакции определено, что передача данных из ГИС в другие системы, которые не обеспечивают должный уровень защиты, запрещена.

В статье 16 Федерального закона, защита информации включает в себя правовые, организационные и технические меры, направленные на:

- защиту данных от несанкционированного доступа, удаления, изменения, блокировки, копирования и других незаконных действий;
- сохранение конфиденциальности информации с ограниченным доступом;
- обеспечение права на доступ к информации.

Требования к защите информации в ГИС и других ИС, устанавливаются федеральной службой безопасности (ФСБ России) и Федеральной службой по техническому и экспортному контролю (ФСТЭК России), в пределах их полномочий. При создании и эксплуатации таких систем используемые методы защиты должны соответствовать этим требованиям.

В соответствии с изложенным, рассмотрим основные требования к защите информационных ресурсов в ГИС, определенные регуляторами.

2. Документом, который существенно изменил требования к защите информации (ЗИ), является **Указ Президента РФ от 1 мая 2022 г. № 250 «О дополнительных мерах по обеспечению информационной безопасности Российской Федерации»**.

Таблица 1.

Перечень новых нормативных правовых документов, определяющих требования по защите государственных информационных ресурсов

№ п/п	Наименование документа	Примечание
1	Федеральный закон от 27 июля 2006 г. № 149-ФЗ «Об информации, информационных технологиях и о защите информации»	Редакция 1 апреля 2025 г.
2	Указ Президента РФ от 1 мая 2022 г. № 250 «О дополнительных мерах по обеспечению информационной безопасности Российской Федерации»	
3	Постановление от 15 июля 2022 г. № 1272 «Об утверждении типового положения о заместителе руководителя органа (организации), ответственном за обеспечение информационной безопасности в органе (организации), и типового положения о структурном подразделении в органе (организации), обеспечивающем информационную безопасность органа (организации)»	
4	Приказ ФСБ России от 18 марта 2025 г. № 117 «Об утверждении Требований о защите информации, содержащейся в государственных информационных системах, иных информационных системах государственных органов, государственных унитарных предприятий, государственных учреждений, с использованием шифровальных (криптографических) средств»	
5	Приказ ФСТЭК России от 11 апреля 2025 № 117 «Об утверждении Требований о защите информации, содержащейся в государственных информационных системах, иных информационных системах государственных органов, государственных унитарных предприятий, государственных учреждений»	В силе с 1 марта 2026 г.
6	Приказ ФСТЭК России от 29.04.2021 № 77 «Об утверждении Порядка организации п проведении работ по аттестации объектов информатизации на соответствие требованиям о защите ограниченного доступа информации, не составляющей государственную тайну»	В ожидании новой редакции
7	Постановление Правительства РФ от 3 ноября 1994 г. № 1233 «Об утверждении Положения о порядке обращения со служебной информацией ограниченного распространения в федеральных органах исполнительной власти, уполномоченном органе управления использованием атомной энергии и уполномоченном органе по космической деятельности»	В редакции от 4 марта 2026 г.
8	Методические рекомендации ФСТЭК России «Состав и содержание мероприятий и мер по защите информации, содержащейся в информационных системах»	Опубликованы 14 апреля 2026 г.

Указ направлен на повышение устойчивости и безопасности работы информационных систем в России. В соответствии с ним на заместителей руководителей организаций возложена ответственность за информационную безопасность, включая выявление и предотвращение компьютерных атак, устранение их последствий и реагирование на инциденты.

Также предписано создавать в организациях отдельные подразделения, которые занимаются вопросами безопасности и выполняют те же задачи. Государственным органам поручено обеспечить выполнение требований данного указа.

Руководителям государственных органов, госкорпораций, стратегических предприятий и других значимых организаций предписано оперативно внедрять организационные и технические меры, которые определяются ФСБ России и ФСТЭК России с учётом актуальных угроз.

Кроме того, установлено, что с 1 января 2025 г. организациям запрещено использовать средства защиты информации иностранного происхождения.

3. Во исполнение Указа, правительством Российской Федерации было принято **Постановление от 15 июля 2022 г. № 1272 «Об утверждении типового положения о заместителе руководителя органа (организации), ответственном за обеспечение информационной безопасности в органе (организации), и типового положения о структурном подразделении в органе (организации), обеспечивающем информационную безопасность органа (организации)»**.

Данный документ определяет, какие полномочия и обязанности есть у заместителя руководителя или другого ответственного лица, которое отвечает за информационную безопасность в государственном органе или организации. В его зону ответственности входит защита систем, а также выявление и устранение последствий компьютерных атак и инцидентов.

К специалисту предъявляются требования в необходимости профильного высшего образования в области информационной безопасности. Если образование получено по другой специальности, требуется дополнительная переподготовка. Также документ описывает его рабочие обязанности, права и ответственность. Он участвует в формировании внутренней политики организации и согласовании её стратегии развития в части безопасности.

Кроме того, утверждено типовое положение о подразделении, которое занимается вопросами информационной безопасности. В нём прописаны его цели, задачи и функции.

Работа подразделения направлена на снижение возможного ущерба от сбоев и атак, защиту конфиденциальных данных, повышение устойчивости организации к внешним и внутренним угрозам, а также обеспечение стабильной и безопасной работы информационных систем и инфраструктуры.

Среди основных задач подразделения:

- планирование и координация мер по защите информации и контроль их выполнения;
- выявление угроз и уязвимостей в системах и программном обеспечении;
- предотвращение утечек данных и несанкционированного доступа;
- поддержание работы организации даже при атаках;
- взаимодействие с профильными государственными центрами;
- обеспечение соблюдения требований законодательства при работе с информацией.

На основе этих задач определены функции подразделения, его права и порядок взаимодействия с другими структурами. Также установлены показатели эффективности работы и ответственность сотрудников за выполнение своих обязанностей.

4. **Приказ ФСБ России от 18 марта 2025 г. № 117 «Об утверждении Требований о защите информации, содержащейся в государственных информационных системах, иных информационных системах государственных органов, государственных унитарных предприятий, государственных учреждений, с использованием шифровальных (криптографических) средств»**.

Анализ содержания рассматриваемых документов показал, что оно незначительно различается, но самое главное, что издание нового документа существенно расширяет круг его действия, что следует из названия. Однако установлено, что данный приказ не касается систем, в которых обрабатываются сведения, составляющие государственную тайну, а также не распространяется на ИС Администрации Президента РФ, Совета Безопасности, Федерального Собрания, Правительства, Конституционного и Верховного судов, а также ФСБ.

Документ устанавливает, что данные в ГИС и других ИС госорганов, предприятий и учреждений должны защищаться с помощью криптографических средств в следующих случаях:

- если по законам Российской Федерации прямо требуется защита информации с использованием криптографии;
- если данные передаются по каналам связи вне охраняемой территории или защищённых помещений;
- если нужно приравнять электронные документы с электронной подписью к бумажным с подписью от руки;
- если информация хранится на носителях, к которым невозможно полностью исключить несанкционированный доступ обычными средствами защиты.

Решение о применении криптографической защиты должно быть обосновано в модели угроз, техническом задании и проектной документации системы.

Модель угроз безопасности информации и (или) техническое задание на создание или развитие ГИС согласуются с ФСБ России в части применения криптографии.

Для защиты информации используются только сертифицированные ФСБ криптографические средства защиты.

Для предотвращения возможных угроз ИБ, направленных на взлом или обход криптозащиты, применяются средства нужного класса, который выбирается в зависимости от значимости данных и масштаба системы (табл. 2).

Порядок определения уровня значимости информации, актуальной угрозы безопасности информации и возможностей источника угроз по осуществлению подготовки и проведению атак, подробно изложены в тексте документа.

5. **Приказ ФСТЭК России от 11.04.2025 № 117 «Об утверждении Требований о защите информации, содержащейся в государственных информационных системах, иных информационных системах государственных органов, государственных унитарных предприятий, государственных учреждений»**.

Таблица 2.

Определение минимально допустимого класса СКЗИ, подлежащих использованию для защиты информации, содержащейся в ИС

Уровень значимости информации	Масштаб ИС		
	ИС (сегмент ИС), предназначенная для решения задач ИС на всей территории Российской Федерации или в пределах двух и более субъектов Российской Федерации	ИС (сегмент ИС), предназначенная для решения задач ИС в пределах одного субъекта Российской Федерации	ИС (сегмент ИС), предназначенная для решения задач ИС в пределах объекта (объектов) одного государственного органа, муниципального образования и (или) организации
Высокий уровень значимости	КВ	КС3	КС2
Средний уровень значимости	КС3	КС3	КС1
Низкий уровень значимости	КС2	КС1	КС1

Документ пришёл на смену приказу ФСТЭК России от 11 февраля 2013 г. № 17, при этом его требования распространяются на более широкий круг информационных систем. В нём описаны меры защиты данных в государственных и связанных с ними системах, предотвращающие вторжения на информационные системы за исключением высших органов власти, а также к системам, связанным с разведкой, контрразведкой и управлением вооружением.

Отмечается, что требования к защите информации стали более строгими. Организация, владеющая системой, должна обеспечивать защиту данных на всех этапах её жизненного цикла от разработки и модернизации до эксплуатации и вывода из работы.

При обеспечении защиты информации, важной целью является снизить риск негативных последствий, связанных как с утечкой или искажением данных, так и с нарушением работы самой системы. Для этого внутри организации должна быть выстроена система работы с безопасностью:

- определены ответственные лица;
- внедрены необходимые программные и технические средства;
- разработаны внутренние правила и выделены ресурсы.

Руководитель организации или назначенное им лицо отвечает за организацию защиты, для этого при необходимости создаётся отдельное подразделение или назначаются специалисты, которые должны обладать нужной квалификацией. При этом часть сотрудников обязана иметь профильное образование или пройти соответствующее обучение.

Работа по защите информации ведётся совместно с другими подразделениями, которые используют и обслуживают систему. Используются инструменты для выявления угроз, мониторинга состояния безопасности, поиска уязвимостей и анализа работы системы.

Внутренние правила и регламенты утверждаются руководством и доводятся до сотрудников и подрядчиков. Управление безопасностью включает планирование мер, их реализацию, оценку текущего состояния и последующее улучшение.

Состояние защиты регулярно оценивается с помощью установленных показателей. Такие проверки проводятся периодически, а их результаты направляются руководству и в уполномоченные органы.

Для защиты информации выполняется комплекс мер: анализ существующих угроз, контроль состояния системы, исправление уязвимостей, проведения систематических обновлений, защита при работе с различными устройствами и каналами доступа, активный мониторинг безопасности, разработка безопасного программного обеспечения, физическая защита и обеспечение устойчивой работы системы при сбоях.

Особое внимание уделяется защите данных ограниченного доступа, для этого фиксируются все активные обращения и контролируется доступ. Также предусмотрены меры по обеспечению непрерывной работы системы и её восстановлению при сбоях, для чего создаются резервные копии и используются отказоустойчивые решения.

Проводится обучение сотрудников, во время которого им объясняют основные правила безопасности, проводят тренировки и проверяют устойчивость к методам социальной инженерии.

Отдельно рассматривается использование технологий искусственного интеллекта, при котором необходимо исключить несанкционированное

влияние на модели и данные, а также применять только проверенные решения.

Выбор мер защиты зависит от уровня значимости системы и предполагаемых возможностей нарушителя. При необходимости могут применяться более строгие меры.

Перед началом работы системы проводится её проверка на соответствие установленным требованиям. В дальнейшем контроль уровня защиты осуществляется регулярно или после инцидентов.

Все меры защиты реализуются с учётом методических рекомендаций ФСТЭК. Защита должна обеспечиваться на всех уровнях от оборудования до прикладных программ и сетевой инфраструктуры.

Используются только сертифицированные средства защиты (табл. 3), соответствующие классу системы. Требования к защите также учитываются на всех этапах жизненного цикла системы от создания до завершения её эксплуатации.

Перечень требуемых мероприятий по выполнению обеспечения защищенности ИС для каждого класса защиты разработан, опубликован 14 апреля 2026 г. и требует изучения и реализации на практике.

6. **Приказ ФСТЭК России от 29.04.2021 № 77 «Об утверждении Порядка организации проведении работ по аттестации объектов информатизации на соответствие требованиям о защите ограниченного доступа информации, не составляющей государственную тайну**».

В данном названии данного документа уже точно обозначены определяемые и разрабатываемые вопросы, Единственное дополнение, что в настоящее время ведется его доработка с учетом новых требований к ГИС.

7. **Постановление Правительства РФ от 3 ноября 1994 г. № 1233 «Об утверждении Положения о порядке обращения со служебной информацией ограниченного распространения в федеральных органах исполнительной власти, уполномоченном органе управления использованием атомной энергии и уполномоченном органе по космической деятельности»**.

Данный документ вышел в новой редакции, которая существенно меняет привычных стиль обращения с документами ограниченного распространения. Во-первых, существенно расширен круг организаций, в которых данные документы могут создаваться и обрабатываться, во-вторых, введено понятие электронный документ и порядок обращения с электронными документами, содержащими информацию ограниченного доступа, а также определены порядок и ответственность должностных лиц за обеспечение защиты документов, данной категории. Это потребует от специалистов систем электронного документооборота, доработки информационных систем и инструкций по их эксплуатации.

Таким образом, на основе анализа требований, вступивших в силу, можно выделить перечень основных направлений по их реализации:

1. Специалистам служб ИБ необходимо изучить Требования к защите ГИС, и определить подпадает ли ИС предприятия под действие рассмотренных документов.
2. Если ИС подпадает под действие данных требований, то необходимо:
   - провести обследование ИС с целью выявления несоответствий уровня защищенности ИС установленным требованиям;
   - разработать эскизный проект системы защиты ИС;
   - составить перечень необходимых средств защиты и заложить в бюджет предприятия соответствующие расходы на приобретение СЗИ и СКЗИ, а также на привлечение сторонних организаций для создания системы защиты;
   - провести аттестацию персонала подразделения ИБ и разработать план повышения квалификации персонала;
   - провести актуализацию нормативных документов предприятия по функционированию ИС и обеспечению безопасности информационных ресурсов в соответствии с установленными требованиями.

По рекомендациям ФСТЭК России разработать план приведения системы защиты в соответствие с Требованиями.

Таблица 3.

Класс защищенности ИС

Уровень значимости информационной системы	Масштаб информационной системы		
	Федеральный	Региональный	Объектовый
УЗ 1	К1	К1	К1
УЗ 2	К1	К2	К2
УЗ 3	К2	К3	К3

В настоящее время можно, с учетом рассмотренных выше требований, приступать к формирования эскизного проекта системы защиты ИС органа государственной власти, предприятия, организации, воинской части.

Выводы

По результатам исследования достигнуты следующие результаты:

1. Проведен краткий анализ требований новых документов, определяющих мероприятия по защите государственных информационных систем. Установлено, что круг информационных систем, подпадающих под действие новых требований существенно расширен и значительное количество должностных лиц подразделений по обеспечению информационной безопасности предприятий обязаны выполнять новые требования. стороны.

2. Система защита государственных информационных ресурсов вышла на новую систему координат, требования к системе защиты носят системный характер и отличаются новыми подходами к организации защиты и новыми критериями оценки их защищенности.

3. Анализ требований показал, что для обеспечения защищенности информационных ресурсов требуется проведение обследования информационных систем, и разработка планов (проектов) приведения систем защиты ИС в соответствие с требованиями, установленными регуляторами.

4. При разработке (модифицировании) системы защиты ГИС следует провести оценку защищенности ГИС по показателям ее защищенности – Кзи и по показателю уровня зрелости – Пзи, и на основе полученных значений формировать систему защиты. Данные показатели эффективности системы защиты являются основными для оценки возможности функционирования ГИС.

5. Очевидно, что к числу основных факторов, затрудняющих обеспечение защиты ИС является отсутствие сертифицированных средств защиты информации и сложности привлечения сторонних организаций для выявления уязвимости ИС, установки СЗИ, СКЗИ и проведения аттестационных испытаний, что объясняется необходимостью существенных финансовых затрат, которые необходимо иметь в бюджете предприятия.

6. Законодательством установлен обязательный перечень нормативных документов, которые должны быть разработаны на предприятии, что необходимо для создания и эксплуатации ГИС. Разработка этого ряда документов требует наличия высоко квалифицированного персонала и, в условиях отсутствия методических материалов, наличия значительного времени.

7. Целесообразно с целью экономии временных ресурсов приступать к разработке типовых документов (форм документов) и методических рекомендаций по их разработке. При этом научным подразделениям Вооруженных сил, уполномоченным на разработку методических документов по обеспечению информационной безопасности целесообразно обеспечить должное взаимодействие с регуляторами.

8. Исходя из значимости обеспечения защиты информационных систем Вооруженных сил и их специфики целесообразно формировать перечень средств обеспечения информационной безопасности, в том числе средств мониторинга событий ИС и/или вырабатывать требования к их разработке.

9. Приведенные в работе документы показывают, что одним из важнейших требований по обеспечению защиты информационных ресурсов является наличие достаточного количества подготовленных специалистов подразделениях технической защиты информации. Опыт показывает не хватку специалистов по информационной безопасности, особенно в государственных организациях. Предлагается учебным заведениям, которые готовят специалистов по работе с информационными системами и защите информации, добавить в учебные программы соответствующие темы, соответствующие требованиям, изложенных в рассмотренных документах.

10. Следует предполагать, что основные существенные требования о защите информационных систем установленные регуляторами должны быть реализованы в большинстве информационных систем Министерства обороны (за исключением оговоренных соответствующими приказами). Очевидно, что эти требования с учетом специфической деятельности необходимо выполнять в Вооруженных силах и необходимо приступать к разработке планов по их реализации.

11. Учитывая трудоемкость мероприятий по защите, ГИС, можно считать целесообразным органам обеспечения информационной безопасности (подразделениям по защите информации) готовиться к их реализации в настоящее время, поскольку соответствующие документы Министерства обороны Российской Федерации будут разработаны на основе документов от регуляторов.

12. В настоящее время разрабатывается новая Доктрина информационной безопасности Российской Федерации и к реализации положений Доктрины необходимо быть готовым, всем структурам, уполномоченным обеспечивать информационную безопасность органов, организаций, предприятий, учреждений и воинских частей.

Литература

1. Волостных В. А. Организация защиты конфиденциальной информации на предприятии средствами криптографической защиты / В. А. Волостных, П. А. Воробьев, В. А. Задбоев // Перспективы безопасности – 2024: Сборник материалов II научно-технической конференции, посвященной информационной безопасности, Санкт-Петербург, 19–20 июня 2024 г. – Санкт-Петербург: ООО «Специальный Технологический Центр», 2024. – С. 9–13.
2. Костарев С. В., Карганов В. В., Липатников В. А., Волостных В. А. Нормативная правовая база Российской Федерации обеспечения информационной безопасности. В книге: технологии защиты информации в условиях кибернетического противоборства. Санкт-Петербург, 2020. – С. 94–158.
3. Викулова А. Ю., Волостных В. А., Кононов П. А., Парфиров В. А. Защита персональных данных территориально-распределенных предприятий. В сборнике: Актуальные проблемы инфотелекоммуникаций в науке и образовании (АПИНО, 2021), сборник научных статей: в 4 т. Санкт-Петербургский государственный университет телекоммуникаций им. проф. М. А. Бонч-Бруевича. СПб., 2021. – С. 155–160.
4. Волостных В. А., Задбоев В. А. Создание систем защищенного электронного документооборота, предназначенных для обработки документов, содержащих информацию ограниченного распространения. В Сборнике трудов конференции Сборник научных статей, 65-я научно-техническая конференция профессорско-преподавательского состава, научных работников и аспирантов (НТК ППС, 2025) СПб., СПбГУТ, 2025. – С 79–84.
5. Викулова А. Ю., Волостных В. А., Кононов П. А., Парфиров В. А. Защита персональных данных территориально-распределенных предприятий. В сборнике: Актуальные проблемы инфотелекоммуникаций в науке и образовании (АПИНО, 2021), сборник научных статей: в 4 т. Санкт-Петербургский государственный университет телекоммуникаций им. проф. М. А. Бонч-Бруевича. СПб., 2021. – С. 155–160.
6. Задбоев В. А. анализ возможностей отечественных средств, применяемых для мониторинга информационной безопасности сетей передачи данных / В. А. Задбоев, Н. А. Роговой, А. А. Шевченко // Актуальные проблемы инфотелекоммуникаций в науке и образовании (АПИНО, 2024): Материалы XIII Международной научно-технической и научно-методической конференции, Санкт-Петербург, 27–28 февраля 2024 года. – СПб.: Санкт-Петербургский государственный университет телекоммуникаций им. проф. М. А. Бонч-Бруевича, 2024. – С. 308-313.
7. Крюкова Е. С. Контроль качества электронных справочных и образовательных ресурсов для подготовки специалистов по техническому обслуживанию и ремонту средств и комплексов автоматизации управления / Е. С. Крюкова, А. Г. Емельяненко, И. Б. Паращук // Проблемы технического обеспечения войск в современных условиях: Труды X Межвузовской научно-практической конференции, Санкт-Петербург, 16 мая 2025 года. – СПб.: Федеральное Государственное Казенное Военное Образовательное Учреждение Высшего Образования «Военная академия связи им. Маршала Советского Союза С. М. Буденного» Министерства Обороны Российской Федерации, 2025. – С. 153–157.
8. Паращук И. Б. Классификационные признаки процедур мониторинга защищенности программно-аппаратных комплексов электронного документооборота, использующих каналы инфокоммуникационных сетей / И. Б. Паращук, Е. С. Владимирова, Л. А. Саяркин // 65-я научно-техническая конференция профессорско-преподавательского состава, научных работников и аспирантов (НТК ППС, 2025) : Сборник научных статей. В 3 т., Санкт-Петербург, 17–21 февраля 2025 года. – СПб.: Санкт-Петербургский государственный университет телекоммуникаций им. проф. М. А. Бонч-Бруевича, 2025. – С. 305–309.
9. Основы построения сертифицированных защищенных баз данных Российской Федерации / А. В. Красов, А. А. Миняев, И. Е. Пестов, И. А. Ушаков. – СПб.: Санкт-Петербургский государственный университет телекоммуникаций им. проф. М. А. Бонч-Бруевича, 2025. – 189 с.
10. Киселев Н. Н. Требования защищённости объекта КИИ с учетом развития требований регуляторов / Н. Н. Киселев, А. В. Красов // Региональная информатика и информационная безопасность: Сборник трудов Санкт-Петербургской международной конференции и XIV Санкт-Петербургской межрегиональной конференции, Санкт-Петербург, 29–31 октября 2025 года. – СПб.: Региональная общественная организация «Санкт-Петербургское Общество информатики, вычислительной техники, систем связи и управления», 2025. – С. 162–165.

ON THE IMPLEMENTATION OF NEW REQUIRED INFORMATION PROTECTION LEGISLATION OF THE RUSSIAN FEDERATION IN STATE INFORMATION SYSTEMS

Volostnykh V. A.[4], Zadboev V. A.[5], Shevchenko A. A.[6]

4 ***Viktor A. Volostnykh***, Ph.D. of Military Sciences, Associate Professor, Researcher of the Military Academy of Communications, St. Petersburg, Russia. E-mail: ra1alo@mail.ru

5 ***Vadim A. Zadboev***, Junior Researcher, Military Academy of Communications, St. Petersburg, Russia. E-mail: zadboev89@mail.ru

6 ***Alexander A. Shevchenko***, Ph.D. of Technical Sciences, Associate Professor, Senior Researcher of the Military Academy of Communications, St. Petersburg, Russia. E-mail: alex_pavel1991@mail.ru

Keywords: *information systems, cryptography, security threats, information security, legal documents.*

Abstract

The purpose of the work: *to analyze the current changes in the requirements for the security of state information systems and to develop approaches to their implementation in modern conditions.*

Results of the study: *changes in the requirements of Russian regulatory documents in the field of information security in state information systems are considered, without affecting information on state secrets.*

Based on the analysis of the modern application of practical experience in the field of information security in organizations, recommendations are proposed for updating protection systems in accordance with innovations. The main problems of the development of security systems of large information systems and ways to solve them are shown, significant changes in the legislation on information protection are identified, proposals are developed to recommend updating protection systems in accordance with innovations, to ensure the security of information processed in the information and telecommunication systems of enterprises, organizations, military units and institutions.

Practical usefulness: *lies in the fact that within the framework of a single study, a systematic documentary comparison of a number of regulatory legal documents is carried out and rational approaches to the implementation of requirements in modern conditions are developed, which can be applied to ensure the security of information in the information systems of enterprises, organizations, military units and institutions.*

References

1. Volostnykh V. A. Organization of the protection of confidential information at the enterprise by means of cryptographic protection / V. A. Volostnykh, P. A. Vorobyov, V. A. Zadboev // Security Prospects – 2024: Collection of materials from the II scientific and technical conference dedicated to information security, St. Petersburg, June 19–20, 2024. – St. Petersburg: OOO «Special Technology Center», 2024. – Pp. 9–13.
2. Kostarev S. V., Karganov V. V., Lipatnikov V. A., Volostnykh V. A. Regulatory legal framework of the Russian Federation for ensuring information security. In the book: Information security technologies in the context of cyber confrontation. St. Petersburg, 2020. – Pp. 94–158.
3. Vikulova A. Yu., Volostnykh V. A., Kononov P. A., Parfirov V. A. Personal data protection of geographically distributed enterprises. In the collection: Actual problems of infotelecommunications in science and education (APINO, 2021), a collection of scientific articles: in 4 volumes. Saint Petersburg State University of Telecommunications named after prof. M. A. Bonch-Bruevich. Saint Petersburg, 2021. – Pp. 155–160.
4. Volostnykh V. A., Zadboev V. A. Creation of secure electronic document management systems designed to process documents containing restricted information. In the Conference Proceedings, Collection of Scientific Articles, 65th Scientific and Technical Conference of Faculty, Researchers, and Postgraduate Students (NTK PPS, 2025), St. Petersburg, SPbSUT, 2025. – Pp. 79–84.
5. Vikulova A. Yu., Volostnykh V. A., Kononov P. A., Parfirov V. A. Personal Data Protection of Geographically Distributed Enterprises. In the collection: Current Issues of Infotelecommunications in Science and Education (APINO, 2021), collection of scientific articles: in 4 volumes. Saint Petersburg State University of Telecommunications named after prof. M. A. Bonch-Bruevich. Saint Petersburg, 2021. – Pp. 155–160.
6. Zadboev V. A. Analysis of the Capabilities of Domestic Tools Used to Monitor the Information Security of Data Transmission Networks / V. A. Zadboev, N. A. Rogovoy, A. A. Shevchenko // Actual Problems of Infotelecommunications in Science and Education (APINO, 2024): Proceedings of the XIII International Scientific, Technical and Scientific-Methodological Conference, Saint Petersburg, February 27–28, 2024. – Saint Petersburg: Saint Petersburg State University of Telecommunications named after prof. M. A. Bonch-Bruevich, 2024. – Pp. 308–313.
7. Kryukova E. S. Quality control of electronic reference and educational resources for training specialists in the maintenance and repair of automation control systems and systems / E. S. Kryukova, A.G. Emelyanenko, I. B. Parashchuk // Problems of technical support of troops in modern conditions: Proceedings of the X Interuniversity Scientific and Practical Conference, St. Petersburg, May 16, 2025. – St. Petersburg: Federal State Treasury Military Educational Institution of Higher Education «Military Academy of Communications named after Marshal of the Soviet Union S. M. Budyonny» of the Ministry of Defense of the Russian Federation, 2025. – P. 153–157.
8. Parashchuk I. B. Classification features of security monitoring procedures for software and hardware complexes of electronic document management using infocommunication network channels / I. B. Parashchuk, E. S. Vladimirova, L. A. Sayarkin // 65th Scientific and Technical Conference of the Faculty, Researchers and Postgraduate Students (NTK PPS, 2025): Collection of scientific articles. In 3 volumes, St. Petersburg, February 17–21, 2025. – St. Petersburg: St. Petersburg State University of Telecommunications named after prof. M. A. Bonch-Bruevich, 2025. – P. 305–309.
9. Fundamentals of constructing certified secure databases of the Russian Federation / A. V. Krasov, A. A. Minyaev, I. E. Pestov, I. A. Ushakov // – Saint Petersburg: Saint Petersburg State University of Telecommunications named after prof. Bonch-Bruevich, 2025. – 189 p.
10. Kiselev N. N. Security requirements for a critical information infrastructure facility, taking into account evolving regulatory requirements / N. N. Kiselev, A. V. Krasov // Regional informatics and information security: Proceedings of the Saint Petersburg International Conference and the XIV Saint Petersburg Interregional Conference, St. Petersburg, October 29–31, 2025. – Saint Petersburg: Regional public organization «Saint Petersburg Society of Informatics, Computer Engineering, Communications and Control Systems», 2025. – pp. 162–165.