/ 5

Государственное учреждение здравоохранения
Ярославской области
«РЫБИНСКАЯ БОЛЬНИЦА № 1»

ПРИКАЗ

от «27» 03 2026 года № 78

Об утверждении политики
защиты информации

В целях исполнения Приказа 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» в государственном учреждении здравоохранения Ярославской области «Рыбинская больница № 1»

П Р И К А З Ы В А Ю:

1. Утвердить прилагаемую «Политику защиты информации» (Приложение № 1).
2. Ознакомить с Политикой руководителей обособленных подразделений.
3. Контроль исполнение приказа оставляю за собой.

Главный врач С.П. Бутаков

КОПИИ НАПРАВИТЬ:
1. Руководителям обособленных подразделений
2. Начальнику информационного отдела
3. Специалисту по защите информации

Исп. Самсонов А.Е. (4855)202-948
Специалист по защите информации

Приложение № 1
к приказу от 27.03.26 № 78

УТВЕРЖДАЮ
Главный врач
ГУЗ ЯО «Рыбинская больница № 1»

_____ С.П. Бутаков

«27» 03 2026 г.

ПОЛИТИКА ЗАЩИТЫ ИНФОРМАЦИИ

государственного учреждения здравоохранения Ярославской области «Рыбинской больницы № 1»

2026

Введение

Политика защиты информации определяет основные цели, задачи и важнейшие принципы деятельности государственного учреждения здравоохранения Ярославской области «Рыбинской больницы № 1» (далее по тексту – ГУЗ ЯО «Рыбинская больница № 1») по вопросам обеспечения безопасности информации, обрабатываемой в информационных системах, информационно-телекоммуникационных сетях (далее по тексту – ИС, ИТКС), в том числе, предотвращения несанкционированного доступа к информации и специальных воздействий на информацию (носители информации) в целях ее добывания, уничтожения, искажения, блокирования к ней доступа и т. п.

Самсонов А.Е.

Перечень сокращений

ЗИ	–	защита информации
ИБ	–	информационная безопасность
ИС	–	информационная система
ИТКС	–	информационно-телекоммуникационная сеть
КИИ	–	критическая информационная инфраструктура
ПДн	–	персональные данные
ПО	–	программное обеспечение
РФ	–	Российская Федерация
СЗИ	–	система защиты информации
СрЗИ	–	средство защиты информации
ТС	–	техническое средство
ФСБ России	–	Федеральная служба безопасности Российской Федерации
ФСТЭК России	–	Федеральная служба по техническому и экспортному контролю Российской Федерации

1 Область действия политики

1.1 Политика представляет собой совокупность управленческих решений, является методологической основой для разработки нормативных и организационно-распорядительных документов в ГУЗ ЯО «Рыбинская больница № 1», регламентирующих правила и нормы обеспечения безопасности информации при ее обработке в информационных системах (включая сбор, систематизацию, накопление, изменение, дополнение, передачу и т. д.).

1.2 Предметами настоящей Политики являются:

– информационные ресурсы, представленные в виде документированной информации на различного рода электронных носителях, информационных массивов и баз данных, подлежащие защите в соответствии с законодательством РФ и внутренними организационно-распорядительными документами ГУЗ ЯО «Рыбинская больница № 1», модификация или утрата которых может привести к нарушению устойчивого функционирования ГУЗ ЯО «Рыбинская больница № 1», его территориальных подразделений;

– персональные данные, их обработка в информационных системах персональных данных, с применением (использованием) различных видов электронных носителей;

– средства и системы информатизации, программные средства, автоматизированные системы управления информационными и технологическими процессами, системы связи и передачи данных, технические средства приема, передачи и обработки информации, используемые для обработки информации ограниченного доступа;

– объекты критической информационной инфраструктуры.

1.3 Выполнение положений Политики является обязательным для всех работников ГУЗ ЯО «Рыбинская больница № 1».

1.4 Выполнение положений Политики является обязательным для работников подрядных организаций, заключивших договор с ГУЗ ЯО «Рыбинская больница № 1», которым в рамках оказания услуг (выполнения работ) необходимо подключение в ИС, ИТКС ГУЗ ЯО «Рыбинская больница № 1».

1.5 Политика обязательна для применения в территориальных подразделениях с целью формирования единых подходов по вопросам информационной безопасности и обеспечения защиты информации.

2 Жизненный цикл политики

2.1 Пересмотр Политики защиты информации ГУЗ ЯО «Рыбинская больница № 1» (далее – Политика) должен производиться в соответствии с учетом результатов контроля состояния ЗИ и соблюдения Политики, а также различных изменений, имеющих отношение к ЗИ.

2.2 Внесение изменений в Политику может производиться на основании:

– изменений в законодательной и нормативной базе по ЗИ, произошедших с момента утверждения предыдущей версии Политики;

– результатов анализа произошедших инцидентов ИБ, а также уязвимостей и угроз, выявленных за время, прошедшее с момента утверждения предыдущей версии Политики;

– результатов контроля состояния ЗИ и предложений подразделений о совершенствовании процедур обеспечения ЗИ;

– изменений в управлении ИБ, включая изменения в распределении ресурсов и обязанностей при обеспечении ЗИ.

3 Цели и задачи обеспечения информационной безопасности ГУЗ ЯО «Рыбинская больница № 1»

3.1 Настоящая Политика определяет следующие ключевые цели.

3.1.1 Защита интересов ГУЗ ЯО «Рыбинская больница № 1» в информационной сфере от всех видов угроз, внешних и внутренних, умышленных и непреднамеренных путем предотвращения или существенного уменьшения вероятности негативного воздействия на информационную инфраструктуру и снижения уровня возможного ущерба субъектам информационных отношений.

3.1.2 Создание условий для реализации прав работников ГУЗ ЯО «Рыбинская больница № 1», его территориальных подразделений на разрешенную законом деятельность в информационной сфере.

Самсонов А.Е.

3.1.3 Установление единых подходов к обеспечению защиты ИС, ИТКС ГУЗ ЯО «Рыбинская больница № 1».

3.1.4 Проведение единой технической политики в области обеспечения ЗИ ГУЗ ЯО «Рыбинская больница № 1», его территориальных подразделений.

3.1.5 Определение методов предотвращения и нейтрализации угроз информационной безопасности.

3.2 В соответствии с целями ставятся следующие задачи информационной безопасности:

– определение угроз, их источников и рисков информационной безопасности;

– определение и обеспечение уровня защищенности ИС, ИТКС в соответствии с требованиями законодательства РФ;

– разработка, внедрение и дальнейшая эксплуатация СЗИ;

– создание механизмов своевременного реагирования на инциденты информационной безопасности;

– разработка внутренних стандартов и регламентов для обеспечения единого подхода к защите информационных ресурсов, определяющих сферу обязанностей и ответственности работников ГУЗ ЯО «Рыбинская больница № 1», обеспечение им беспрепятственного доступа к информационным ресурсам необходимым для выполнения должностных обязанностей;

– определение перечня мероприятий, направленных на контроль состояния ЗИ;

– проведение мероприятий по оценке состояния защищенности информации;

– проведение мероприятий по повышению уровня знаний и осведомленности пользователей ИС, ИТКС;

– проведение мероприятий по проверке знаний работников в сфере информационной безопасности.

4 Принципы реализации Политики

4.1 Политика основывается на следующих принципах:

– соблюдение Конституции и законодательства Российской Федерации, общепризнанных норм международного права, а также отраслевых / ведомственных нормативных документов;

– правовое равенство всех участников процесса информационного взаимодействия при обработке информации любым законным способом;

– соблюдение баланса интересов личности, ГУЗ ЯО «Рыбинская больница

№ 1» и государства в информационной сфере;

– обеспечение безопасности ГУЗ ЯО «Рыбинская больница № 1» при создании ИС, их эксплуатации и защите содержащейся в них информации;

– установление ИТКС ограничений доступа к информации только в соответствии с федеральными законами РФ;

– обеспечение свободы поиска, получения, передачи, производства и распространения информации любым законным способом;

– осуществление обработки ПДн на законной и справедливой основе;

– сбор исключительно необходимых, соответствующих целям обработки, ПДн, а также применение организационно-технических мер по обеспечению их безопасности;

– обработка только тех ПДн, которые отвечают целям их обработки;

– гарантия соответствия содержания и объема обрабатываемых ПДн заявленным целям обработки. Недопущение избыточности ПДн по отношению к заявленным целям их обработки;

– обеспечение точности, достаточности и актуальности по отношению к целям обработки ПДн;

– обеспечение хранения ПДн в форме, позволяющей определить субъекта ПДн, не дольше, чем этого требуют цели обработки ПДн, если срок хранения ПДн не установлен федеральным законом, договором, стороной которого, выгодоприобретателем или поручителем по которому является субъект ПДн;

– гарантия непрерывного и комплексного обеспечения безопасности значимых объектов КИИ;

– гарантия достоверности информации и своевременность ее предоставления.

5 Общие положения

5.1 Основу Политики составляют:

– централизованная разработка документов ГУЗ ЯО «Рыбинская больница № 1», регламентирующих вопросы ИБ, обязательность выполнения их требований;

– персональная ответственность за нарушения в сфере ИБ;

– обеспечение постоянного контроля состояния ЗИ в ГУЗ ЯО «Рыбинская больница № 1».

5.2 Политику разрабатывает и представляет на утверждение специалист по защите информации Информационно-аналитического отдела А.Е. Самсонов.

5.3 Политика утверждается Главным врачом.

5.4 Ответственность за внедрение и поддержание Политики в актуальном

Самсонов А.Е.

состоянии несет Самсонов А.Е., специалист по защите информации.

6 Заинтересованные стороны

6.1 В реализации Политики внутри организации участвуют следующие работники ГУЗ ЯО «Рыбинская больница № 1»:

– руководители структурных подразделений ГУЗ ЯО «Рыбинская больница № 1»;

– владельцы информационных активов (руководители подразделений ГУЗ ЯО «Рыбинская больница № 1», отвечающих за информационный актив);

– администраторы ИС, ИТКС, осуществляющие техническую поддержку информационных ресурсов;

– пользователи информационных ресурсов (работники ГУЗ ЯО «Рыбинская больница № 1», работники подрядных организаций, а также сторонние пользователи, подключающиеся к информационной инфраструктуре ГУЗ ЯО «Рыбинская больница № 1» с помощью веб-ресурсов (при наличии)).

6.2 Внешнее сотрудничество.

6.2.1 Взаимоотношения по использованию положений данного документа применительно к ЗИ, находящейся в совместном ведении с другими организациями, регулируются на основании специальных соглашений.

6.2.2 Взаимоотношения по использованию положений данного документа применительно к ЗИ, к которой предоставляется доступ для работников подрядных организаций, заключивших договор с ГУЗ ЯО «Рыбинская больница № 1» на оказание услуг (выполнение работ) в ИС, ИТКС, регулируются на основании специальных соглашений

6.2.3 Взаимодействие с государственными органами РФ регулируется действующим законодательством и локальными нормативными актами ГУЗ ЯО «Рыбинская больница № 1».

6.2.4 Политика считается реализованной, в части взаимодействия заинтересованных сторон, если:

– участники процесса соблюдают ее положения;

– организовано административное регулирование процессов по обеспечению требуемого уровня защищенности информационных активов;

– оптимизированы затраты на обеспечение ЗИ на различных этапах жизненного цикла информационных активов.

7 Угрозы и источники угроз информационной безопасности

7.1 Под угрозой ИБ понимается совокупность условий и факторов, создающих потенциальную или реально существующую опасность

несанкционированных и / или непреднамеренных воздействий на информацию.

7.2 Угрозы ИБ по их функциональной направленности подразделяются на:

– угрозы конфиденциальности информации, предусматривающие перехват информации, хищение, утрату информации или ее носителей;

– угрозы целостности информации – преднамеренное умышленное и неумышленное искажение (модификацию) информации;

– угрозы доступности информации – преднамеренное умышленное и неумышленное уничтожение, блокирование доступа к информации или средствам её обработки.

7.3 Политикой рассматриваются внешние и внутренние источники угроз ИБ ГУЗ ЯО «Рыбинская больница № 1».

7.4 Внешними источниками угроз ИБ ГУЗ ЯО «Рыбинская больница № 1» являются:

– Внешние пользователи, не имеющие права доступа до информационных ресурсов.

7.5 Внутренними источниками угроз ИБ ГУЗ ЯО «Рыбинская больница № 1» являются:

– Внутренние пользователи, имеющие доступ до информационных ресурсов.

8 Риски информационной безопасности

8.1 Рисками ИБ являются:

– Операционный риск – риск, возникающий в результате недостатков в организации деятельности, используемых технологиях, функционировании информационных систем, неадекватных действий или ошибок сотрудников, а также в результате внешних событий.

– Информационный риск (ИТ - риск, риск автоматизации процессов) – риск, связанный с использованием информационных технологий, неудовлетворительным состоянием автоматизированных систем;

– Риск информационной безопасности – риск, являющийся составной частью ИТ - риска, возникающий вследствие наличия угроз безопасности информационным активам.

9 Организационные вопросы защиты информации

9.1 ЗИ организовывает руководитель ГУЗ ЯО «Рыбинская больница № 1» или ответственное лицо по его решению.

9.2 Руководитель ГУЗ ЯО «Рыбинская больница № 1» или ответственное лицо назначает отдельных специалистов, на которых возлагаются обязанности по ЗИ.

Самсонов А.Е.

9.3 Ответственные специалисты обеспечивают защиту информации во взаимодействии с подразделениями (работниками), использующими ИС, ИТКС, и подразделениями (работниками), обеспечивающими эксплуатацию ИС, ИТКС.

9.4 Подразделения (работники), использующие ИС, ИТКС, участвуют в проведении мероприятий и принятии мер по обеспечению ЗИ в объеме, установленном во внутренних стандартах и регламентах по ЗИ.

9.5 Подразделения, обеспечивающие эксплуатацию ИС, ИТКС, проводят мероприятия и принимают меры по ЗИ в ходе сопровождения, обслуживания ИС, ИТКС поставки комплектующих и иных видов работ по эксплуатации ИС, ИТКС в объеме, установленном во внутренних стандартах и регламентах по ЗИ ГУЗ ЯО «Рыбинская больница № 1».

9.6 Ответственными специалистами применяются программные, программно-аппаратные средства, позволяющие обеспечить выполнение возложенных на них обязанностей по ЗИ.

9.7 Для проведения мероприятий и принятия мер по ЗИ руководством ГУЗ ЯО «Рыбинская больница № 1» могут привлекаться организации, имеющие лицензию на деятельность по технической ЗИ ограниченного доступа (далее – лицензиат). Состав проводимых специализированными организациями мероприятий и принимаемых ими мер по ЗИ, используемых при этом программных, программно-аппаратных средств, предназначенных для обеспечения ЗИ, определяется ответственными специалистами. Ответственные специалисты должны привлекаться к приемке результатов работ и услуг, выполняемых специализированными организациями.

9.8 Ответственные специалисты разрабатывают и представляют ответственному лицу обоснованные предложения по организационным, материально-техническим и иным обеспечивающим ресурсам, необходимым для проведения мероприятий и принятия мер по ЗИ, с указанием сведений о целях ЗИ, на достижение которых требуются ресурсы, и перечня негативных последствий, наступление которых прогнозируется в случае отсутствия ресурсов.

9.8.1 Ответственное лицо на основе представленных предложений и в пределах имеющихся средств предусматривает выделение организационных, материально-технических и иных обеспечивающих ресурсов для проведения мероприятий и принятия мер по ЗИ, привлечения при необходимости дополнительных сил и средств для защиты информации на всех этапах жизненного цикла ИС, ИТКС.

9.9 В рамках управления деятельностью по ЗИ ответственным специалистам по ЗИ необходимо обеспечить решения следующих задач:

- разработка и планирование мероприятий по ЗИ;
- проведение мероприятий и принятие мер по ЗИ;

– проведение оценки состояния защищенности информации;

– совершенствование мероприятий и мер по ЗИ.

10 Управление рисками информационной безопасности

10.1 Управление рисками ИБ осуществляется путем реализации следующих мер ЗИ и ИС, ИТКС.

10.1.1 Обеспечение безопасности при идентификации и аутентификация субъектов доступа и объектов доступа посредством:

– идентификации и аутентификации пользователей, работниками ГУЗ ЯО «Рыбинская больница № 1», не являющихся работниками ГУЗ ЯО «Рыбинская больница № 1», а также пользователей, подключающихся к информационной инфраструктуре ГУЗ ЯО «Рыбинская больница № 1» с помощью веб ресурсов (при наличии);

– управления идентификаторами, в том числе создания, присвоения, уничтожения идентификаторов;

– управления средствами аутентификации, в том числе хранения, выдачи, инициализации, блокирования средств аутентификации и принятия мер в случае утраты и (или) компрометации средств аутентификации;

– защиты обратной связи при вводе аутентификационной информации;

– определения объектов файловой системы, запускаемых и исполняемых модулей, объектов систем управления базами данных, объектов, создаваемых прикладным и специальным программным обеспечением, а также иных объектов доступа, подлежащих аутентификации в случае необходимости.

10.1.2 Управление доступом субъектов доступа к объектам доступа включает в себя:

– управление (заведение, активация, блокирование и уничтожение) учетными записями пользователей, в том числе внешних пользователей;

– реализацию необходимых методов (дискреционный, мандатный, ролевой или иной метод), типов (чтение, запись, выполнение или иной тип) и правил разграничения доступа;

– управление (фильтрация, маршрутизация, контроль соединений, однонаправленная передача и иные способы управления) информационными потоками между устройствами, сегментами информационной системы, а также между ИС, ИТКС;

– разделение полномочий (ролей) пользователей, администраторов и лиц, обеспечивающих функционирование ИС, ИТКС;

– назначение минимально необходимых прав и привилегий пользователям, администраторам и лицам, обеспечивающим функционирование ИС, ИТКС;

Самсонов А.Е.

– ограничение неуспешных попыток входа в ИС;

– блокирование сеанса доступа в ИС после установленного времени бездействия (неактивности) пользователя или по его запросу;

– разрешение (запрет) действий пользователей, разрешенных до идентификации и аутентификации;

– реализацию защищенного удаленного доступа субъектов доступа к объектам доступа через внешние ИТКС;

– регламентацию и контроль использования в ИС, ИТКС технологий беспроводного доступа;

– регламентацию и контроль использования в ИС, ИТКС мобильных технических средств;

– управление взаимодействием с ИС, ИТКС сторонних организаций (внешние информационные системы).

10.1.3 В ИС, ИТКС применяются следующие меры по ограничению программной среды:

– установка (инсталляция) только разрешенного к использованию ПО и (или) его компонентов.

10.1.4 Деятельность по защите машинных носителей информации включает в себя:

– учет машинных носителей информации;

– управление доступом к машинным носителям информации;

– уничтожение (стирание) информации на машинных носителях при их передаче между пользователями, в сторонние организации для ремонта или утилизации, а также контроль уничтожения (стирания).

10.1.5 Деятельность по регистрации событий безопасности состоит из:

– определения событий безопасности, подлежащих регистрации, и сроков их хранения;

– определения состава и содержания информации о событиях безопасности, подлежащих регистрации;

– сбора, записи и хранения информации о событиях безопасности в течение установленного времени хранения;

– реагирования на сбои при регистрации событий безопасности, в том числе аппаратные и программные ошибки, сбои в механизмах сбора информации и достижение предела или переполнение объема (емкости) памяти;

– мониторинга (просмотр, анализ) результатов регистрации событий безопасности и реагирования на них;

– генерирования временных меток и (или) синхронизации системного времени в информационной системе;

– защиты информации о событиях безопасности.

10.1.6 При реализации антивирусной защиты необходимо обеспечить обновление базы данных признаков вредоносных компьютерных программ (вирусов).

10.1.7 Процесс контроля (анализа) защищённости информации состоит из следующих этапов:

– выявление, анализ уязвимостей ИС, ИТКС и оперативное устранение вновь выявленных уязвимостей;

– контроль установки обновлений ПО, включая обновление ПО СрЗИ;

– контроль работоспособности, параметров настройки и правильности функционирования ПО и СрЗИ;

– контроль состава ТС, ПО и СрЗИ;

– контроль правил генерации и смены паролей пользователей, заведения и удаления учетных записей пользователей, реализации правил разграничения доступом, полномочий пользователей в ИС, ИТКС.

10.1.8 Обеспечение целостности ИС, ИТКС и информации осуществляется посредством:

– возможности восстановления ПО, включая ПО СрЗИ, при возникновении нештатных ситуаций.

10.1.9 Обеспечение доступности информации осуществляется с помощью следующих шагов:

10.1.10 Защита среды виртуализации реализовывается с помощью:

– идентификации и аутентификации субъектов доступа и объектов доступа в виртуальной инфраструктуре, в том числе администраторов управления средствами виртуализации;

– управления доступом субъектов доступа к объектам доступа в виртуальной инфраструктуре, в том числе внутри виртуальных машин;

– регистрации событий безопасности в виртуальной инфраструктуре;

– реализации и управления антивирусной защитой в виртуальной инфраструктуре;

– разбиения виртуальной инфраструктуры на сегменты (сегментирование виртуальной инфраструктуры) для обработки информации отдельным пользователем и (или) группой пользователей.

10.1.11 Защита ТС включает следующие меры:

Самсонов А.Е.

– организация контролируемой зоны, в пределах которой постоянно размещаются стационарные ТС, обрабатывающие информацию, и СрЗИ, а также средства обеспечения функционирования;

– контроль и управление физическим доступом к ТС, СрЗИ, средствам обеспечения функционирования ИС, ИТКС, а также в помещения и сооружения, в которых они установлены, исключающие несанкционированный физический доступ;

– размещение устройств вывода (отображения) информации, исключающее ее несанкционированный просмотр.

10.1.12 Защита ИС, ИТКС и их средств, систем связи и передачи данных включает в себя:

– обеспечение защиты информации от раскрытия, модификации и навязывания (ввода ложной информации) при ее передаче (подготовке к передаче) по каналам связи, имеющим выход за пределы контролируемой зоны, в том числе беспроводным каналам связи;

– запрет несанкционированной удаленной активации видеокамер, микрофонов и иных периферийных устройств, которые могут активироваться удаленно, и оповещение пользователей об активации таких устройств;

– защита беспроводных соединений, применяемых в ИС, ИТКС;

– защита мобильных ТС, применяемых в ИС, ИТКС.

11 Ответственность в сфере информационной безопасности

11.1 Установление ответственности.

11.1.1 Обязанности работник не должны совмещать (в любой комбинации) функции разработки, сопровождения, исполнения, администрирования и контроля.

11.1.2 На руководителей самостоятельных подразделений ГУЗ ЯО «Рыбинская больница № 1» возлагаются обязанности по обеспечению соблюдения установленного порядка обращения с информацией ограниченного доступа.

11.1.3 Все работники ГУЗ ЯО «Рыбинская больница № 1» дают письменное обязательство о неразглашении информации, содержащей конфиденциальные сведения, в том числе сведения, составляющие служебную тайну, находящиеся в распоряжении ГУЗ ЯО «Рыбинская больница № 1».

11.1.4 Каждый работник ГУЗ ЯО «Рыбинская больница № 1», имеющий доступ к сведениям, не подлежащим разглашению сведениям, несет ответственность за их разглашение и утрату, а также за нарушение установленного порядка обеспечения информационной безопасности.

11.1.5 Работники ГУЗ ЯО «Рыбинская больница № 1», разгласившие конфиденциальную информацию или нарушившие установленный порядок

обращения с ней, а также работники, по вине которых произошла утрата конфиденциальных документов, несут ответственность, предусмотренную законодательством Российской Федерации и внутренними документами ГУЗ ЯО «Рыбинская больница № 1».

11.2 Порядок контроля.

11.2.1 Контроль соблюдения требований ИБ в ГУЗ ЯО «Рыбинская больница № 1», территориальных подразделениях осуществляется с целью определения соответствия принятых мер по защите информации нормативно-правовым актам, а также внутренним стандартам и регламентам ГУЗ ЯО «Рыбинская больница № 1».

11.2.2 Контроль осуществляется ответственными специалистами по ЗИ при выполнении:

– плановых проверок;

– внеплановых проверок состояния защиты информации в ГУЗ ЯО «Рыбинская больница № 1», территориальных подразделениях по указанию руководителя ГУЗ ЯО «Рыбинская больница № 1»;

– постоянного мониторинга состояния защищенности ИС, ИТКС.

11.2.3 Контроль состояния защищенности ИС, ИТКС осуществляется путем интервьюирования руководителей и работников структурных подразделений, анализа документации, осуществления инструментальных проверок.

11.2.4 Результаты проведения контроля состояния ИБ документируются.

Самсонов А.Е.

Перечень используемых документов

1. Конституция Российской Федерации.

2. Федеральный закон Российской Федерации от 27.07.2006 № 149-ФЗ «Об информации, информационных технологиях и о защите информации».

3. Федеральный закон Российской Федерации от 29.07.2004 № 98-ФЗ «О коммерческой тайне».

4. Федеральный закон Российской Федерации от 27.07.2006 № 152-ФЗ «О персональных данных».

5. Федеральный закон Российской Федерации от 26.07.2017 № 187-ФЗ «О безопасности критической информационной инфраструктуры Российской Федерации».

6. Приказ ФСТЭК России от 11.04.2025 № 117 «О защите информации, содержащейся в государственных информационных системах, иных информационных системах государственных органов, государственных унитарных предприятий, государственных учреждений».

7. Приказ ФСТЭК России от 21.12.2017 № 235 «Об утверждении Требований к созданию систем безопасности значимых объектов критической информационной инфраструктуры Российской Федерации и обеспечению их функционирования».

8. Приказ ФСТЭК России от 25.12.2014 № 239 «Об утверждений Требований по обеспечению безопасности значимых объектов критической информационной инфраструктуры Российской Федерации».

9. Приказ ФСБ России от 18.03.2025 № 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».

10. Приказ ФСБ России от 24.07.2018 № 368 «Об утверждении Порядка обмена информацией о компьютерных инцидентах между субъектами критической информационной инфраструктуры Российской Федерации, между субъектами критической информационной инфраструктуры Российской Федерации и уполномоченными органами иностранных государств, международными, международными неправительственными организациями и иностранными организациями, осуществляющими деятельность в области реагирования на компьютерные инциденты, и Порядка получения субъектами критической информационной инфраструктуры Российской Федерации информации о средствах и способах проведения компьютерных атак и о методах их предупреждения и обнаружения».

11. Приказ ФСБ России от 10.07.2014 № 378 «Об утверждении Состава и содержания организационных и технических мер по обеспечению безопасности персональных данных при их обработке в информационных системах персональных данных с использованием средств криптографической защиты информации, необходимых для выполнения установленных Правительством Российской Федерации требований к защите персональных данных для каждого из уровней защищенности».

12. Приказ ФСТЭК России от 18.02.2013 № 21 «Состав и содержание организационных и технических мер по обеспечению безопасности персональных данных при их обработке в информационных системах персональных данных».

Исполнитель:
Самсонов А.Е.
Специалист по защите информации
(4855)202-948

Самсонов А.Е.