Министерство цифрового развития Вологодской области

ПРИКАЗ

«6 »ноября 2026 года № 101-О

Об утверждении Методических рекомендаций по выполнению требований по защите информации, содержащейся в государственных информационных системах, иных информационных системах в органах исполнительной государственной власти области, государственных учреждениях области

В целях реализации 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» и на основании постановления Правительства Вологодской области от 09.07.2025 № 990 «Об осуществлении полномочий исполнительных органов области по обеспечению информационной безопасности»

ПРИКАЗЫВАЮ

1. Утвердить прилагаемые Методические рекомендации по выполнению требований по защите информации, содержащейся в государственных информационных системах, иных информационных системах в органах исполнительной государственной власти области государственных учреждениях области (далее – Методические рекомендации).

2. Ознакомить с Методическими рекомендациями руководителей исполнительных органов области и подведомственных им учреждений, обеспечивающие функций в сфере информационных технологий которых переданы в соответствии с постановлениями Губернатора области бюджетному учреждению в сфере информационных технологий Вологодской области «Центр информационных технологий (далее – органы/учреждения).

3. Настоящий приказ вступает с даты его официального опубликования.

Заместитель Губернатора –
министра цифрового развития области А.А. Ильина

УТВЕРЖДЕНЫ
приказом Министерства цифрового развития области
от «6» ноября 2026 г. №101-0

Методические рекомендации
по выполнению требований
по защите информации, содержащейся в государственных информационных системах, иных информационных системах
в органах исполнительной государственной власти области, государственных учреждениях области (далее – Методические рекомендации)

1. Настоящие Методические рекомендации разработаны в целях защиты информации в соответствии с Требованиями о защите информации, содержащейся в государственных информационных системах, иных информационных системах государственных органов, государственных унитарных предприятий, государственных учреждений, утвержденными приказом ФСТЭК России от 11 апреля 2025 г. № 117 (далее – Требования, Регулятор), методическим документом «Состав и содержание мероприятий и мер по защите информации, содержащейся в информационных системах», утвержденным ФСТЭК России 12 апреля 2026 г., и определяют перечень организационных мероприятий, которые рекомендуется реализовать в органах исполнительной государственной власти (далее – органы) и подведомственных им учреждениях (далее – учреждения) Вологодской области.

2. Настоящие Методические рекомендации предназначены для исполнительных органов области и подведомственных им учреждений (далее – органы, учреждения), обеспечивающие функций в сфере информационных технологий которых переданы в соответствии с постановлениями Губернатора области (далее – органы/учреждения) бюджетному учреждению в сфере информационных технологий Вологодской области «Центр информационных технологий (далее – БУ ВО «ЦИТ»), подведомственному учреждению Министерства цифрового развития Вологодской области.

Применение положений настоящих Методических рекомендаций в отношении исполнительных органов области и подведомственных им учреждений осуществляется с учетом особенностей их деятельности, в части, не противоречащей целям и видам деятельности, определенным нормативно-правовыми актами или уставами учреждений.

3. Исполнительным органам области и подведомственным им учреждениях в целях реализации Требований рекомендуется:

3.1. При реализации Требований, а также сопровождении представителей ведомств, уполномоченных на контроль исполнения Требований, руководствоваться Приложением 1 к настоящим Методическим рекомендациям.

3.2. В соответствии с пунктом 13, подпунктом «а» пункта 14 Требований разработать и утвердить в исполнительном органе области/учреждении политику защиты информации (далее - Политика), учитывая специфику деятельности и

наличие у органа/учреждения обязанностей и функций в соответствии с Требованиями и схемой взаимодействия и прилагаемой типовой формой Политики (Приложение 2 к Методическим рекомендациям).

В случае внесения органом/учреждением изменений в типовую форму политики при ее утверждении, политика органа/учреждения подлежит согласованию с Министерством цифрового развития области.

3.3. Принять к сведению, что для органов/учреждений внутренние стандарты по защите информации соответствующими подпункту «г» пункта 14 Требований и применимыми к информационной инфраструктуре Правительства области и размещенным в ней информационным системам и ресурсам, являются внутренние стандарты по защите информации, разрабатываемые и утверждаемые Министерством цифрового развития Вологодской области (далее – Стандарты).

3.4. Разработать в соответствии с подпунктом «д» пункта 14 Требований (актуализировать при наличии) внутренние регламенты (инструкции) по защите информации в органе/учреждении, учитывающие функции, исполняемые работниками органа/учреждения для защиты информации, в том числе:

- порядок предоставления сотрудникам иных организаций (пользователям) доступа к информационным системам, оператором информационной системы (обладателем информации) которых является соответствующий орган/учреждение, если такой порядок не определен положениями о соответствующих информационных системах;

- порядок обработки хранения и обращения с информацией ограниченного доступа, если такой порядок не определен иными инструкциями (в т.ч. разработанными в соответствии с «Методические рекомендации по защите информации на автоматизированных рабочих местах, предназначенных для обработки служебной информации ограниченного распространения в органах исполнительной государственной власти области, государственных учреждениях области», утвержденными Министерством цифрового развития области);

- порядок доступа в помещения органа/организации, организации мер физической защиты в них, если такой порядок не установлен в иных документах, договорах с собственниками таких помещений;

- порядок обеспечения выполнения пользователями значимых функций в случае превышения интервалов времени восстановления используемых информационных систем, в том числе в неавтоматизированном режиме;

- порядок инструктирования сотрудников органа/учреждения, повышения их уровня знаний и информированности в вопросах информационной безопасности.

Внутренние регламенты (инструкции) по защите информации органов/учреждений согласовать с Министерством цифрового развития области.

3.5. Ознакомить сотрудников органа/учреждения с утвержденной в органе/учреждении политикой защиты информации, Стандартами и утвержденными в органе/учреждении внутренними регламентами (инструкциями) по защите информации, указанными в пунктах 3.2-3.4 настоящих Методических рекомендаций.

Приложение 1
к Методическим рекомендациям

Участники и порядок их взаимодействия
при организации защиты информации в органах/учреждениях,
обеспечивающие ИТ-функции которых переданы подведомственному учреждению Министерства цифрового развития Вологодской области в соответствии с постановлениями Губернатора области

1. Правовые основания

- Федеральный закон от 27.07.2006 № 149-ФЗ «Об информации, информационных технологиях и о защите информации»;
- Федеральный закон от 27.07.2006 № 152-ФЗ «О персональных данных»;
- Постановление Правительства РФ от 06.07.2015 N 676 «О требованиях к порядку создания, развития, ввода в эксплуатацию, эксплуатации и вывода из эксплуатации государственных информационных систем и дальнейшего хранения содержащейся в их базах данных информации»;
- Постановление Правительства РФ от 01.11.2012 N 1119 «Об утверждении требований к защите персональных данных при их обработке в информационных системах персональных данных»;
- 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»;
- Методический документ «Состав и содержание мероприятий и мер по защите информации, содержащейся в информационных системах» (утв. ФСТЭК России 12.04.2026)
- Постановление Правительства Вологодской области от 09.07.2025 № 990 «Об осуществлении полномочий исполнительных органов области по обеспечению информационной безопасности»
- ГОСТ Р ИСО/МЭК 27002-2021 «Информационные технологии. МЕТОДЫ И СРЕДСТВА ОБЕСПЕЧЕНИЯ БЕЗОПАСНОСТИ. Свод норм и правил применения мер обеспечения информационной безопасности».

2. Термины и определения

На всех (любых) стадиях жизненного цикла каждой информационной системы должна быть обеспечена защита информации в ней. В контексте данного документа выделены основные стадии: создание (внедрение) информационной системы и ее эксплуатация.

Эксплуатация информационной системы —этап жизненного цикла информационной системы, который начинается после её ввода в эксплуатацию (формально данное событие фиксируется соответствующим актом) и включает комплекс мероприятий по обеспечению стабильной, безопасной и эффективной работы системы в соответствии с её целевым назначением.

Для государственных информационных систем их эксплуатация без соответствующего акта ввода в эксплуатацию ограничена постановлением Правительства РФ от 06.07.2015 г. №676. Так как для иных информационных систем аналогичных требований не предусмотрено, порядок их ввода в эксплуатацию определяется внутренними документами оператора информационной системы, при эксплуатации негосударственной информационной системы не допускается игнорирование правовых, организационных и технических требований к обеспечению функционирования и защите информации в ней.

Данный раздел направлен на исключение ситуаций неопределенности/отсутствия лиц, ответственных за организацию мер защиты в системе на какой-либо из стадий.

Для стадии создания (внедрения) информационных систем в федеральных нормах, указанных в разделе 1, предусмотрены соответствующие понятия и роли.

Обладатель информации – лицо (или орган/учреждение), самостоятельно создавшее информацию либо получившее на основании закона или договора право разрешать или ограничивать доступ к информации. Обладатель информации обязан принимать меры по защите информации, ограничивать доступ к информации, если такая обязанность установлена федеральными законами, а также соблюдать права и законные интересы иных лиц. Обладатель информации вправе разрешать или ограничивать доступ к информации, определять порядок и условия такого доступа. Обладатель информации может не иметь достаточных компетенций в ИТ-технологиях и обычно выступает «Функциональным заказчиком» для органа/учреждения, которое непосредственно обеспечивает приобретение или создание информационной системы по заявке Обладателя информации.

Технический заказчик (далее - Заказчик) - Министерство цифрового развития области и (или) его подведомственные учреждения, которые в соответствии с постановлением Губернатора области о передаче обеспечивающих ИТ-функций и/или на основании государственного контракта организуют работы по созданию либо развитию информационной системы, включая систему защиты информации. Технический заказчик обеспечивает реализацию мер защиты информации на этапе создания (внедрения) информационной системы и исполняет обязанности по защите информации до момента утверждения Оператора ИС в соответствии с положением об информационной системе или иным правовым актом.

При этом, следует учитывать соотношение терминов «заказчик...», используемых в нормативных правовых актах (в частности в постановлении Правительства РФ от 06.07.2015 № 676 и ФСТЭК России):

а) Заказчик создания системы (в соответствии с разделом VII ПП РФ от 06.07.2015 № 676) — орган государственной власти, принимающий решение о создании, развитии или модернизации государственной информационной системы. В настоящих Методических рекомендациях этому понятию соответствует Обладатель информации (орган/учреждение).

б) Заказчик (в соответствии с Требованиями приказов ФСТЭК России от 11.04.2025 № 117, от 11.02.2013 № 17) — лицо, заключающее контракт на

создание информационной системы и обеспечивающее разработку и внедрение системы защиты информации. В настоящих Методических рекомендациях этому понятию соответствует Технический заказчик (далее — Заказчик) — Министерство цифрового развития области и (или) его подведомственные учреждения.

Таким образом, настоящие Методические рекомендации используют термин «Технический заказчик» (Заказчик) для отнесения к лицу, указанному в Требованиях ФСТЭК России, и не подменяет собой понятие «заказчик создания системы» из постановления Правительства РФ т 06.07.2015 № 676.

На этапе эксплуатации информационной системы регуляторы используют термин «оператор информационной системы».

Оператор информационной системы (Оператор ИС) – лицо (или орган/учреждение), осуществляющее деятельность по эксплуатации информационной системы (обеспечивающее ее эксплуатацию), в том числе по обработке информации, содержащейся в её базах данных.

Если иное не установлено федеральными законами, Оператором ИС является собственник используемых для обработки содержащейся в базах данных информации технических средств, который правомерно пользуется такими базами данных, или лицо, с которым этот собственник заключил договор об эксплуатации информационной системы.

Регулятором также предусмотрены дополнительные роли/участники:

Уполномоченные лица:

Обработчик - лицо (или орган/учреждение), обрабатывающее информацию, являющуюся информационным ресурсом, по поручению Обладателя информации или Оператора ИС;

Владелец инфраструктуры - лицо (или орган/учреждение), предоставляющее Обладателю информации, Заказчику или Оператору ИС вычислительные ресурсы (мощности) для обработки информации на основании заключенного договора;

Разработчик (проектировщик) – лицо (или орган/учреждение), привлекаемое в соответствии с законодательством Российской Федерации для проведения работ по созданию (проектированию) информационных систем в защищенном исполнении и (или) их систем защиты информации.

Уполномоченный орган оператора — Министерство цифрового развития области и (или) его подведомственные учреждения, осуществляющие технические функции по эксплуатации информационных систем и технической защите информации в интересах Оператора ИС на основании постановления Правительства Вологодской области от 09.07.2025 № 990 и постановления Губернатора области о передаче обеспечивающих ИТ-функций, а также положений о соответствующих информационных системах.

Схематично описанные выше роли/участники, представлены на рис.1., при этом стрелками обозначены предусмотренные взаимоотношения (договоры/заявки), в т.ч. на создание системы (=>Заказчику), обработку информации (=>Обработчику) или на вычислительные мощности (=>Владельцу инфраструктуры).

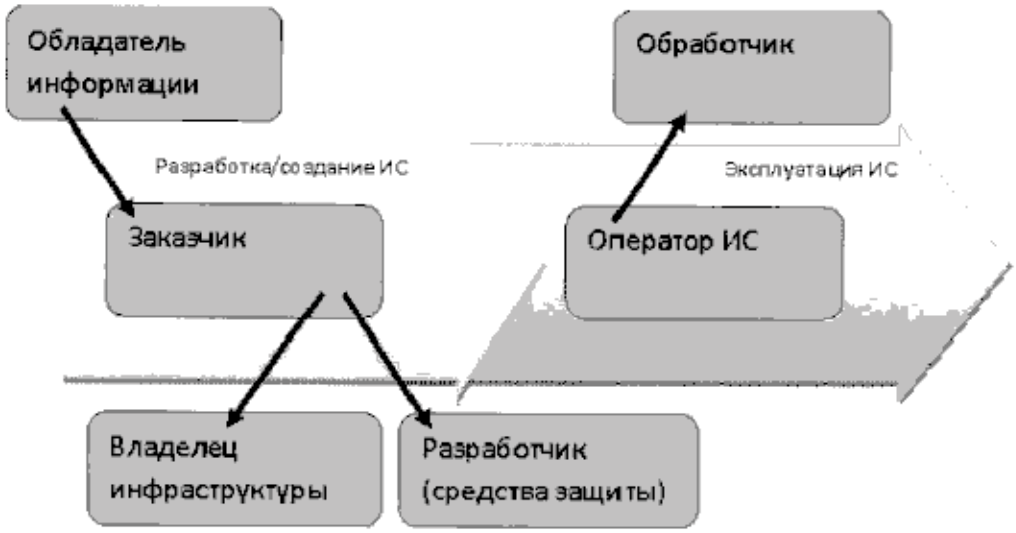


Рис.1

При этом обязанности Обладателя информации и/или Заказчика по защите информации кроме прочего предусматривают:

- Формирование требований к защите информации, содержащейся в информационной системе. При этом учитываются положения политик обеспечения информационной безопасности не только Обладателя информации (Заказчика), а также политик обеспечения информационной безопасности Оператора ИС и уполномоченных лиц в части, не противоречащей политикам Обладателя информации (Заказчика).

- Разработка системы защиты информации. При этом проектная документация на информационную систему и (или) ее систему защиты информации подлежат согласованию с Оператором ИС в случае, если он определен таковым в соответствии с законодательством Российской Федерации к моменту окончания проектирования системы защиты информации в информационной системе и не является Заказчиком данной информационной системы.

- Внедрение системы защиты информации. При этом внедрение системы защиты информации информационной системы осуществляется в соответствии с проектной и эксплуатационной документацией на систему защиты информации информационной системы и в том числе включает разработку документов, определяющих правила и процедуры, реализуемые Оператором ИС для обеспечения защиты информации в информационной системе в ходе ее эксплуатации (далее - организационно-распорядительные документы по защите информации).

Таким образом, меры защиты, разрабатываемые и реализуемые Обладателем информации и/или Заказчиком на этапе создания и внедрения системы обеспечивают принципиальное требование регуляторов – обеспечение необходимых мер защиты (испытание и ввод системы защиты в эксплуатацию) до момента фактического начала эксплуатации информационной системы (до начала обработки в ней защищаемой информации).

Следует отметить, что для этапа эксплуатации Обладатель информации обычно предлагается (подразумевается) в качестве будущего Оператора создаваемой информационной системы. Тем не менее, до момента его назначения (принятия соответствующего положения) обязанности по защите должны быть исполнены Обладателем информации и/или Заказчиком.

3. Распределение ролей в инфраструктуре Правительства Вологодской области

С учетом постановлений Губернатора области о передаче обеспечивающих ИТ-функций, органом уполномоченным на выполнение части функций Обладателя информации и Оператора ИС является Министерство цифрового развития области и ему подведомственные учреждения.

Для государственных информационных систем эта особенность учитывалась в соответствующих положениях о государственных информационных системах (в соответствии со статьей 13 закона 149-ФЗ, особенности эксплуатации государственных информационных систем могут устанавливаться в соответствии с техническими регламентами, нормативными правовыми актами государственных органов, принимающих решения о создании таких информационных систем).

В данном разделе уточняются участники, ответственные за мероприятия по защите информационных систем, порядок их определения/назначения, а также их задачи/обязанности в соответствии с действующими требованиями для Обладателя информации, Заказчика, Оператора ИС и уполномоченных лиц, указанных в разделе 2.

Министерство цифрового развития области, исполняя возложенные полномочия, для всех (любых) информационных систем, размещенных в информационной инфраструктуре Правительства области, определяет и доводит до заинтересованных лиц информацию статусе, жизненной стадии информационной системы и о лицах (учреждениях), исполняющих функции Обладателя информации, Заказчика, а также Оператора ИС и уполномоченных лиц.

На рис.2 схематично указанны роли/участники с учетом полномочий Министерства цифрового развития и его подведомственных учреждений.

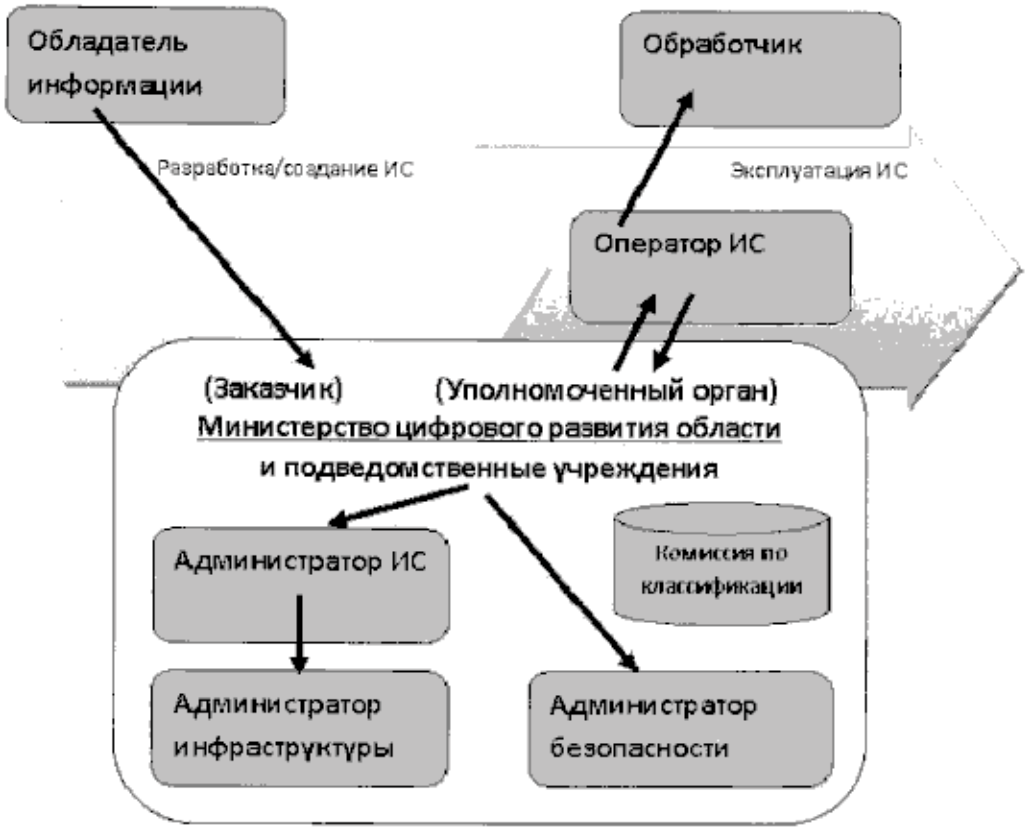


Рис.2

Органы/учреждения, в случае передачи их обеспечивающих функций в сфере информационных технологий подведомственному учреждению Министерства цифрового развития Вологодской области в соответствии с постановлениями Губернатора области и чьи информационные системы размещены в информационной инфраструктуре Правительства области, при реализации мер защиты информации в них выступают в ролях Обладатель информации и/или Оператор ИС.

В свою очередь Министерство цифрового развития и его подведомственные учреждения для информационных систем, размещенных в инфраструктуре Правительства области:

- реализуют функции Заказчика на этапе создания внедрения информационных систем;

- реализуют функции Уполномоченного органа оператора на этапе эксплуатации указанных информационных систем.

При этом Администратором инфраструктуры и Администратором безопасности являются ответственные лица (подразделения) в БУ ВО «Центр информационных технологий», соответственно предоставляющие/обеспечивающие вычислительные мощности и подсистему/средства защиты для информационных систем; Администраторами ИС назначается ответственные лица (или подразделение) в БУ ВО «Центр информационных технологий» или БУ ВО «Электронный регион» (по решению учредителя), обеспечивающие закупку и функционирование информационной системы (прикладного ПО).

Также по решению Министерства цифрового развития подведомственное учреждение БУ ВО «Центр информационных технологий» может быть определено Заказчиком и Уполномоченным органом оператора для информационных систем учреждений, подведомственным исполнительным органам области.

4. Распределение функций при исполнении Требований

В данном разделе определены основные типовые задачи и функции непосредственно органов/учреждений, являющихся Обладателями информации и Операторами ИС, с учетом функций Министерства цифрового развития области и подведомственных учреждений (функций Заказчика и функций Уполномоченного органа оператора).

Полный перечень задач и функций Обладателя информации, Оператора для конкретной информационной системы и в соответствии с текущими требованиями к защите информации определяет (при необходимости) Министерство цифрового развития области. Кроме того, в данном документе не приводится описание распределения иных задач и функций между учреждениями, подведомственными Министерству цифрового развития области.

В соответствии с пунктом 2 Требований ФСТЭК России от 11.04.2025 № 117 обязанности по защите информации возлагаются на оператора (обладателя информации) как единого адресата. Передача технических функций по эксплуатации информационных систем и технической защите информации Уполномоченному органу оператора не освобождает Оператора ИС (орган/учреждение) от ответственности за выполнение требований.

Распределение функций между Оператором ИС и Уполномоченным органом оператора подлежит закреплению в соглашении о взаимодействии либо вытекает из соотвествующих постановлений о передаче функций.

4.1. Основные типовые функции Обладателя информации (Органы/учреждения):

- обеспечить наличие в органе/учреждении политики защиты информации;
- обеспечить участие полномочного представителя органа/учреждения в заседании Комиссии по классификации информационных систем области (при классификации соответствующей информационной системы и определении уровня защищенности персональных данных в ней);
- обеспечить контроль выполнения мер защиты со стороны Уполномоченного органа оператора;
- информировать Уполномоченный орган оператора об изменениях в составе обрабатываемой информации, могущих повлиять на уровень защиты.

4.2. Основные типовые функции Заказчика (Министерства цифрового развития области и его подведомственных учреждений), соответствующие понятию «заказчик», используемому в Требованиях ФСТЭК России:

- обеспечить классификацию информационной системы и определение уровня защищенности персональных данных в ней или принять участие в заседание Комиссии по классификации информационных систем области (в

соответствии с приказом Министерства цифрового развития области от 20.02.2026 №12-О);

- обеспечить разработку и внедрением мер защиты информации;
- обеспечить подготовку акта ввода системы в эксплуатацию;
- исполнять обязанности Оператора ИС до его определения/назначения.

4.3. Основные типовые функции Оператора ИС (Органы/учреждения):

- утвердить положение об информационной системе, при этом закрепить за собой статус Оператора ИС;
- обеспечить оформление акта ввода системы в эксплуатацию, если ввод в эксплуатацию не был определен ранее;
- обеспечить наличие в органе/учреждении политики защиты информации;
- утвердить документы, разработанные Заказчиком или Уполномоченным органом оператора во исполнение требований к защите информационной системы;
- обеспечить меры защиты в отношении используемых помещений;
- актуализировать мероприятия по контролю защиты информации в информационной системе в планах внутреннего контроля;

4.4. Основные типовые функции Уполномоченного органа оператора системы (Министерство цифрового развития области и его подведомственные учреждения):

- участие в разработке положения об информационной системе;
- актуализация организационно-распорядительной документации для системы;
- обеспечить контроль наличия необходимых мер защиты, их эффективность (аттестацию для государственных информационных систем).

4.5. В случаях, когда в информационной системе предусмотрена обработка персональных данных (далее — ПД), Оператором персональных данных в смысле Федерального закона № 152-ФЗ является Обладатель информации (орган/учреждение), определяющий цели обработки ПД, их состав и действия (операции), совершаемые с ними.

Оператор ИС (и уполномоченные лица), осуществляющий техническую обработку ПД в информационной системе, но не определяющий цели, состав и действия с ПД, не является оператором ПД в части определения целей и состава обработки. Таким образом в части, касающейся технической обработки и обеспечения защиты ПД, Оператор ИС несёт обязанности, установленные Федеральным законом № 152-ФЗ и постановлением Правительства РФ от 01.11.2012 № 1119, лишь как лицо, осуществляющее обработку ПД.

Перечень дополнительных к п. 4.1 и 4.3 типовых функций для Оператора персональных данных (Органы/учреждения):

- Определить ответственное лицо за организацию обработки персональных данных в информационной системе;

- Дополнить инструкцию ответственного за организацию обработки персональных данных сведениями о новой ИСПДн (при необходимости);
- Разработать (или актуализировать) документ об оценке вреда, который может быть причинен субъектам персональных данных в случае нарушения Федерального закона «О персональных данных»;
- Внести изменения в существующие документы органа/учреждения, определяющие политику, локальные акты по вопросам обработки ПД, в т.ч. перечень должностей, замещение которых предусматривает осуществление обработки ПД либо осуществление доступа к ИСПДн;
- Уведомить Роскомнадзор об изменениях в обработке ПД органом/учреждением;
- Обеспечить ведение (создать) журналов об ознакомлении работников органа/учреждения, непосредственно осуществляющих обработку ПД, с положениями законодательства Российской Федерации о ПД, а также локальными актами по вопросам обработки ПД.
- Обеспечить реализацию технических мер защиты персональных данных в информационной системе силами Уполномоченного органа оператора в соответствии с установленным уровнем защищённости;
- Обеспечить контроль за соблюдением мер защиты персональных данных со стороны Уполномоченного органа оператора.

5. Ответственность участников при распределении ролей

5.1. В соответствии с Требованиями ФСТЭК России обязанности по защите информации возлагаются на оператора (обладателя информации) как на единого адресата. При распределении ролей между несколькими органами/учреждениями:

— Обладатель информации несёт ответственность за определение состава защищаемой информации, утверждение модели угроз, контроль выполнения мер защиты;

— Оператор ИС несёт ответственность за утверждение положения о системе, наличие политики защиты, классификацию системы, контроль выполнения мер защиты;

— Заказчик (Технический заказчик) несёт ответственность за обеспечение защиты на этапе создания, включая разработку проектной документации на систему защиты и внедрение мер защиты;

— Уполномоченный орган оператора несёт ответственность за техническую реализацию мер защиты, аттестацию системы, актуализацию модели угроз, расчёт показателей защищённости, реагирование на инциденты, взаимодействие с ГосСОПКА.

5.2. Распределение функций не освобождает ни одного из участников от обязанности по обеспечению защиты информации.

Приложение 2 к Методическим
рекомендациям

Начало формы

УТВЕРЖДАЮ
Руководитель органа/учреждения облас

_____ И.О. Фамилия

«___» _____ 202__ г.

Политика защиты информации
органа/учреждения области **(далее - Организация)**

1. Общие положения

1.1. Правовую основу Политики защиты информации (далее — Политика) составляют законы Российской Федерации и другие нормативно-правовые акты, определяющие права, обязанности и ответственность физических и юридических лиц, публичных образований в сфере информационной безопасности, а также нормативные, отраслевые и ведомственные документы, в том числе:

- Федеральный закон от 27.07.2006 № 149ФЗ «Об информации, информационных технологиях и о защите информации»;
- Федеральный закон от 27.07.2006 № 152ФЗ «О персональных данных»;
- Требования о защите информации, содержащейся в государственных информационных системах, иных информационных системах государственных органов, государственных унитарных предприятий, государственных учреждений, утвержденными приказом ФСТЭК России от 11 апреля 2025 г. N 117;
- иные нормы и методические документы в области информационной безопасности.

1.2. Настоящая Политика не является полным описанием системы защиты информации, в том числе не содержит описания правил и процедур настройки и эксплуатации средств защиты информации. Политика применяется для организации, совершенствования и развития системы обеспечения информационной безопасности.

1.3. Термины и определения:

Информация — сведения (сообщения, данные) независимо от формы их представления;

Защищаемая информация — информация, подлежащая защите в соответствии с требованиями нормативных правовых актов или требованиями, устанавливаемыми Обладателем информации;

Информационная система — совокупность содержащейся в базах данных информации и обеспечивающих её обработку информационных технологий и технических средств;

2. Область действия политики защиты информации

2.1. Настоящая Политика распространяется на:

- Все виды информации в Организации, которые подлежат защите.

- Информационные системы и ресурсы Организации, программно-аппаратные средства вычислительной техники, используемые сотрудниками Организации для обработки и хранения информации;

- Процессы обработки информации в Организации — сбор, хранение, передача, использование, уничтожение данных;

- Физические объекты, связанные с обработкой информации — помещения Организации, где размещены рабочие места, хранилища данных и т. п..

- Сотрудников всех структурных подразделений Организации;

- Внешних лиц, взаимодействующих с информационными системами Организации. К ним относятся подрядчики, партнёры, поставщики, клиенты и другие третьи лица, которые получают доступ к информации в системах или информационным ресурсам Организации.

2.2. Положения настоящей Политики применимы для использования во внутренних нормативных и методических документах, а также в договорах и соглашениях с контрагентами.

3. Объекты защиты

3.1. Информация — любые данные независимо от формы их представления (тексты, числа, изображения, аудио- и видеоматериалы), в т.ч. персональные данные, коммерческая тайна, служебная информация, конфиденциальные документы, данные о технологиях, финансовых операциях и другие категории.

3.2. Информационные системы, Оператором ИС (Обладателем информации) которых является Организация:

- _____
- _____
- _____

А также иные информационные системы, используемые сотрудниками Организации.

3.3. Технические и программные средства, в том числе рабочие станций, мобильные устройства, средства защиты, используемые сотрудниками Организации для обработки, хранения и передачи информации.

3.4. Помещения, которыми на законных основаниях пользуется Организация и в которых размещается технические и программные средства, используемые для обработки, хранения и передачи информации.

4. Цели и задачи политики защиты информации

4.1. Цели:

- исключение утечки информации ограниченного доступа;

- предотвращение несанкционированного доступа, модификации, подмены, удаления информации;

- недопущение использования информационных систем не по назначению;

- исключение распространения противоправной информации;

- недопущение (снижения возможности) наступления негативных последствий при нарушении функционирования информационных систем.

4.2 Задачи:

- управление рисками и угрозами, в том числе оценка информационных активов Организации, определение их критичности;
- определение требований к защите информации;
- обеспечение защиты при обработке, хранении и передаче информации;
- соблюдение требований законодательства и стандартов;
- инструктаж и повышение осведомлённости пользователей.

5. Принципы и стратегии защиты информации

5.1. Используемые принципы:

- Комплексность и непрерывность. Защита информации достигается через согласованное взаимодействие технических, организационных и административных мер.
- Риск-ориентированный подход. Меры защиты должны быть пропорциональны уровню риска.
- Ответственность. Каждый сотрудник несёт ответственность за соблюдение требований ИБ в пределах своих функциональных обязанностей.
- Законность. Должно быть обеспечено соблюдение требований законодательства РФ в области защиты информации.

5.2. Стратегия защиты и обеспечения информационной безопасности в Организации заключается в использовании заранее разработанных мер противодействия угрозам, а также в использовании программно-технических и организационных решений, позволяющих свести к минимуму возможные потери от технических аварий и ошибочных действий персонала.

Необходимо учитывать, что с течением времени меняется характер угроз, поэтому следует своевременно, используя данные мониторинга и аудита, обновлять модели угроз и нарушителя.

6. Организация управления деятельностью по защите информации

6.1. Настоящий раздел описывает структуру органов управления для инициирования и контроля внедрения, а также функционирования защиты информации в Организации.

6.2. Защита информации в Организации является частью комплекса мер системы управления информационной безопасностью в информационной инфраструктуре Правительства области, исполнительных органов области и государственных учреждений области. Система управления информационной безопасностью включает политики, стандарты, регламенты, технические и организационные меры, направленные на защиту информации.

6.3. Структура управления защитой информации в информационной инфраструктуре Правительства области, исполнительных органов области и государственных учреждений области с описанием ключевых функций:

6.3.1. **Министерство цифрового развития** области – утверждение внутренних стандартов защиты информации, координация и контроль выполнения мероприятий по обеспечению информационной безопасности.

6.3.2. **Руководитель Организации** (и/или назначенные им ответственные лица) — организация, координация и контроль соблюдения организационных мер защиты информации.

Для информационных систем, в которых Организация является Оператором ИС, руководитель Организации или уполномоченное им лицо (ответственный за защиту) организует выполнение Пользователями ИС мер по защите информации при эксплуатации, а также контроль мер защиты информации.

Результаты контроля отражаются в журнале учета мероприятий по контролю обеспечения защиты информации при ее обработке в ИС в соответствии с регламентом-инструкцией ответственным за защиту информации в ИС . Выявленные факты нарушений расследуются в соответствии с регламентом-порядком проведения служебных расследований

6.3.3. **Руководители подразделений Организации** — обеспечение выполнения требований защиты информации сотрудниками.

Первичный инструктаж лица, допущенного к защищаемым информационным ресурсам, проводит его непосредственный руководитель в соответствии с регламентом организации первичного инструктажа.

6.3.4. **Учреждения подведомственные Министерству цифрового развития области** – реализация мер защиты в соответствии с внутренними стандартами и регламентами (инструкциями) защиты информации, в том числе:

1) управляют учётными записями;

2) контролируют доступ к ресурсам, обеспечивают предотвращение несанкционированного доступа к информации и (или) передачи ее лицам, не имеющим права на доступ к информации;

3) организуют постоянный контроль за обеспечением уровня защищенности информации, а также контролируют работоспособность, параметры настройки и правильности функционирования ПО и средств защиты;

4) проводят мониторинг и аудит, в том числе обеспечивают своевременное обнаружение фактов несанкционированного доступа к информации, а также предупреждение возможности неблагоприятных последствий нарушения порядка доступа к информации;

5) организуются меры, направленные на выявление (поиск), анализ и устранение уязвимостей, обеспечивают обновление программного обеспечения и средств защиты;

6) реагируют на инциденты, обеспечивают возможность незамедлительного восстановления информации, модифицированной или уничтоженной вследствие несанкционированного доступа к ней;

7) обеспечивают резервирование программного обеспечения и информации, обрабатываемой в ИС;

8) осуществляют учет технических средств ИС, а также порядок вывода их из обращения;

9) реализуют иные организационные и технические меры по технической защите информации (в части, касающейся серверного оборудования и функционирования ППО).

Указанные меры защиты информации в информационной инфраструктуре Правительства области и размещенных в ней ИС реализуются в рамках соответствующих им системам защиты в зависимости от класса защищенности ИС, угроз безопасности информации, структурно-функциональных характеристик ИС, применяемых информационных технологий и особенностей функционирования ИС.

Кроме того, совместно с Оператором ИС реализуются мероприятия по повышению уровня знаний и информированности пользователей ИС, включающие:

- доведение информационных материалов, в том числе НПА в сфере защиты информации, НПА по защите, инструкций пользователя ИС, памяток, баннеров, буклетов, по актуальным вопросам защиты информации;
- проведение лекций, семинаров, обучающих игр по вопросам защиты информации;
- проведение имитационных рассылок электронных писем на служебные адреса электронной почты, иные служебные средства коммуникаций с целью оценки устойчивости пользователей к методам социальной инженерии;
- в системе дистанционного обучения и других системах обучение вопросам защиты информации и безопасной работе с информационными технологиями.

6.4. Управление деятельностью по защите информации включает:

- Разработку и планирование мероприятий и мер по защите информации, включая анализ рисков, определение требований к защите, разработку регламентов и процедур;

- Проведение мероприятий и реализация технических и организационных мер по защите информации;

- Проведение оценки состояния защиты информации, аудит системы защиты и проверка соответствия требованиям;

- Совершенствование мероприятий и мер по защите информации, в том числе обновление политик, процедур, технических средств.

6.5. Для обеспечения эффективности защиты информации внедряются механизмы контроля и отчётности:

- Проводятся внутренние и внешние аудиты для оценки соответствия мер и системы защиты установленным требованиям и стандартам;

- Регулярные совещания по вопросам информационной безопасности;

- Отчёты о состоянии информационной безопасности, результатах аудитов, инцидентах и мерах по их устранению.

7. Категории лиц в Организации, участвующих в защите и их обязанности

7.1. Общее руководство обеспечением защиты информации осуществляет руководитель Организации:

- утверждает Политику;

- утверждает внутренние регламенты защиты информации для сотрудников Организации;

- обеспечивает выполнение организационных мероприятий по защите информации;

- выделяет ресурсы для защиты информации в рамках своих полномочий;

- организует доведение требований защиты информации до сотрудников иных организаций, имеющих доступ к информационным системам и ресурсам (в том числе подрядным организациям), а также обеспечивает их выполнение;

- назначает ответственных лиц для выполнения указанных выше обязанностей;

7.2. Руководители структурных подразделений Организации несут ответственность за обеспечение выполнения требований информационной безопасности в своих подразделениях.

Руководители обеспечивают обучение и повышение осведомленности сотрудников: вводный инструктаж при трудоустройстве, регулярные тренинги, тестирование знаний, информирование о новых угрозах и способах самозащиты.

7.3. Сотрудники учреждения обязаны соблюдать порядок обращения с конфиденциальными документами, носителями ключевой информации и другой защищаемой информацией, соблюдать требования настоящей Политики и других документов, регламентирующих защиту информации, в том числе:

- защищают свои учётные данные;
- используют только разрешённое ПО;
- сообщают о подозрительных событиях.

8. Ответственность сотрудников

8.1. За нарушение требований Политики, а также установленных правил обработки информации, сотрудники несут дисциплинарную, гражданскую, административную и уголовную ответственность согласно нормам действующего законодательства.

8.2. Нарушения требований по обеспечению зашиты информации и их последствия по значимости разделяются на категории.

8.2.1. Нарушения I категории, к которым относятся нарушения, повлекшие за собой разглашение (утечку), уничтожение (искажение) защищаемой информации и/или утрату машинных носителей информации, выведение из строя технических и программных средств, в том числе:

- несанкционированный доступ к защищаемой информации;
- организация утечки сведений;
- умышленное нарушение работоспособности системы.

8.2.2. Нарушения II категории, к которым относятся нарушения, в результате которых возникают предпосылки к разглашению (утечке), уничтожению (искажению) защищаемой информации, утрате машинных носителей информации, выведению из строя технических и программных средств, в том числе:

- утрата учтенного машинного носителя информации;
- многократная неудачная попытка входа под чужим именем, паролем;
- удачная попытка входа под чужим именем, паролем;

- несанкционированное копирование защищаемой информации на внешние носители информации;
- несанкционированная установка (удаление) программного обеспечения;
- неумышленное заражение компьютерными вирусами.

8.2.3. Нарушения III категории, к которым относятся нарушения, не несущие признаков нарушений I и II категорий, в том числе:

- периодическая попытка неудачного доступа к информации;
- нецелевое использование средств вычислительной техники и информационных ресурсов.

8.3. По выявленным фактам нарушений I и II категорий проводится служебная проверка.

9. Заключительные положения

9.1. Политика действует бессрочно и подлежит плановой и/или внеплановой актуализации. Плановая актуализация настоящей политики производится ежегодно и имеет целью приведение в соответствие определенных политикой мер реальным условиям и текущим требованиям к защите информации. Внеплановая актуализация политики информационной безопасности производится в обязательном порядке в следующих случаях:

- при изменении политики РФ в области информационной безопасности, указов и законов РФ в области защиты информации;

- при изменении внутренних нормативных документов (стандартов, регламентов, инструкций, положений), касающихся информационной безопасности Организации;

- при происшествии и выявлении инцидента (инцидентов) по нарушению информационной безопасности, влекущего ущерб.

9.2. Все изменения и дополнения к Политике утверждаются приказом руководителя Организации.

9.3. Сотрудники Организации обязаны ознакомиться с Политикой под подпись.

9.4. Контроль за исполнением требований настоящей политики и поддержанием ее в актуальном состоянии возлагается на _____.