КОМИТЕТ ИНФОРМАЦИОННЫХ ТЕХНОЛОГИЙ
ВОЛГОГРАДСКОЙ ОБЛАСТИ
(ОБЛКОМИНФОРМТЕХНОЛОГИИ)

ПРИКАЗ

15 мая 2026 г. № 69-о/д

г. Волгоград

Об утверждении Регламента по обеспечению информационной безопасности в органах исполнительной власти Волгоградской области

В соответствии с распоряжением Губернатора Волгоградской области от 22 июля 2022 г. № 157-р "О Политике информационной безопасности в органах исполнительной власти Волгоградской области":

1. Утвердить прилагаемый Регламент по обеспечению информационной безопасности в органах исполнительной власти Волгоградской области (далее – Регламент).

2. Заведующему сектором цифрового государственного управления и контроля информационной безопасности комитета информационных технологий Волгоградской области:

довести настоящий приказ до сведения органов исполнительной власти Волгоградской области;

осуществлять контроль за соблюдением органами исполнительной власти Волгоградской области положений Регламента.

3. Контроль за исполнением приказа возложить на заместителя председателя комитета В.А. Заварухина.

4. Настоящий приказ вступает в силу со дня подписания и подлежит официальному опубликованию.

Председатель комитета А.А.Некина

УТВЕРЖДЕН
приказом комитета
информационных технологий
Волгоградской области
от "15" мая 2026 г. № 69-о/д

РЕГЛАМЕНТ
по обеспечению информационной безопасности в органах исполнительной власти Волгоградской области

1. Термины и определения

В настоящем регламенте по обеспечению информационной безопасности в органах исполнительной власти Волгоградской области используются следующие термины и определения:

Автоматизированная система – система, состоящая из персонала и комплекса средств автоматизации его деятельности, реализующая информационную технологию выполнения установленных функций (далее - АС);

Автоматизированное рабочее место – программно-технический комплекс АС, предназначенный для автоматизации деятельности определённого вида;

Аутентификация – совокупность мероприятий по проверке лица на принадлежность ему идентификатора (идентификаторов) посредством сопоставления его (их) со сведениями о лице, которыми располагает лицо, проводящее аутентификацию, и установлению правомерности владения лицом идентификатором (идентификаторами) посредством использования аутентифицирующего (аутентифицирующих) признака (признаков) в рамках процедуры аутентификации, в результате чего лицо считается установленным;

Идентификация – совокупность мероприятий по установлению сведений о лице и их проверке, осуществляемых в соответствии с федеральными законами и принимаемыми в соответствии с ними нормативными правовыми актами, и сопоставлению данных сведений с уникальным обозначением (уникальными обозначениями) сведений о лице, необходимыми для определения такого лица (далее — идентификатор);

Безопасность информации – состояние защищённости информации, при котором обеспечены её конфиденциальность, доступность и целостность;

Владелец информационных ресурсов, информационных систем, технологий и средств их обеспечения – субъект, осуществляющий владение и пользование указанными объектами и реализующий полномочия распоряжения в пределах своей компетенции;

Государственная информационная система – информационная система, создаваемая в целях реализации полномочий органов исполнительной власти Волгоградской области по обеспечению обмена информацией между ними, а также в иных случаях, установленных положениями законодательства (далее – ГИС);

Документ – зафиксированная на материальном носителе информация с реквизитами, позволяющими её идентифицировать;

Доступность информации – состояние, характеризующееся способностью обеспечивать беспрепятственный доступ к информации субъектов, имеющих на это полномочия;

Защита информации – деятельность, направленная на предотвращение утечки защищаемой информации, несанкционированных и непреднамеренных воздействий на защищаемую информацию;

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

Информационная безопасность – состояние защищённости личности, общества и государства от внутренних и внешних информационных угроз, при котором обеспечиваются реализация конституционных прав и свобод человека и гражданина, достойные качество и уровень жизни граждан, суверенитет, территориальная целостность и устойчивое социально-экономическое развитие Российской Федерации, оборона и безопасность государства (далее – ИБ);

Информационная система – совокупность содержащейся в базах данных информации и обеспечивающих её обработку информационных технологий и технических средств (далее – ИС);

Информационный ресурс – отдельные документы и отдельные массивы документов, документы и массивы документов в информационных системах, на дисках серверов органов исполнительной власти Волгоградской области, в базах данных, в электронной почте (далее – ИР);

Информация ограниченного доступа – информация, которая подлежит защите согласно положениям действующего законодательства;

Инцидент информационной безопасности – появление одного или нескольких нежелательных или нежданных событий ИБ, с которыми связана значительная вероятность компрометации операций и создания угрозы ИБ;

Контролируемая зона – пространство (территория, здание, часть здания), в котором исключено неконтролируемое пребывание лиц, а также транспортных, технических или иных средств;

Конфиденциальность информации – обязательное для выполнения лицом, получившим доступ к определённой информации, требование не передавать такую информацию третьим лицам без согласия её обладателя;

Несанкционированный доступ – доступ к информации или к ресурсам автоматизированной информационной системы, осуществляемый

с нарушением установленных прав и (или) правил доступа;

Оператор информационной системы – гражданин или юридическое лицо, осуществляющие деятельность по эксплуатации информационной системы, в том числе по обработке информации, содержащейся в её базах данных;

Пароль – средство проверки личности пользователя для доступа к ИС или сервису, обеспечивающее идентификацию и аутентификацию на основе сведений, известных только пользователю;

Процесс – последовательность технологически связанных операций по предоставлению продуктов, услуг и (или) осуществлению конкретного вида деятельности органа исполнительной власти Волгоградской области;

Риск – сочетание вероятности события и его последствий;

Сеть управления и передачи данных Волгоградской области – комплексная система, обеспечивающая информационный обмен между органами исполнительной власти Волгоградской области, а также иными организациями, действующими на территории Волгоградской области (далее - СУПД);

Система управления информационной безопасностью – часть общей системы управления, основанная на оценке рисков, предназначенная для создания, внедрения, эксплуатации, мониторинга, анализа, сопровождения и совершенствования (далее – СУИБ);

Собственник информационных ресурсов, информационных систем, технологий и средств их обеспечения – субъект, в полном объёме реализующий полномочия владения, пользования, распоряжения указанными объектами;

Угроза – опасность, предполагающая возможность потерь (ущерба);

Целостность информации – устойчивость информации к несанкционированному доступу или случайному воздействию на неё в процессе обработки техническими средствами, результатом которого может быть уничтожение и искажение информации;

Шифрование – криптографический метод, который может использоваться для обеспечения защиты информации ограниченного доступа.

2. Общие положения

2.1. Настоящий Регламент разработан в соответствии с федеральными законами от 27 июля 2006 г. № 149-ФЗ "Об информации, информационных технологиях и о защите информации", от 27 июля 2006 г. № 152-ФЗ "О персональных данных", Указом Президента Российской Федерации от 17 марта 2008 г. № 351 "О мерах по обеспечению информационной безопасности Российской Федерации при использовании информационно-телекоммуникационных сетей международного информационного обмена, Распоряжением Губернатора Волгоградской области от 22 июля 2022 г. № 157-р "О политике информационной

безопасности в органах исполнительной власти Волгоградской области а также иными федеральными нормативными правовыми актами и нормативными правовыми актами Волгоградской области.

2.2. Положения Регламента применяются в отношении всех процессов в сфере ИБ в органах исполнительной власти Волгоградской области (далее – ОИВ) и являются обязательными для использования сотрудниками ОИВ.

2.3. Регламент определяет цели обеспечения информационной безопасности, объекты защиты обеспечения информационной безопасности, принципы обеспечения информационной безопасности и основные мероприятия, направленные на обеспечения информационной безопасности.

3. Цели обеспечения информационной безопасности являются

3.1. Основными целями обеспечения информационной безопасности являются:

своевременное выявление, оценка и прогнозирование источников угроз ИБ;

создание механизма оперативного реагирования на угрозы ИБ;

предотвращение и (или) снижение ущерба от реализации угроз ИБ;

защита от вмешательства в процесс функционирования ИС, АС посторонних лиц;

обеспечение непрерывности протекающих процессов;

достижение адекватности мер по защите от угроз ИБ;

создание на региональном уровне эффективного механизма межведомственного взаимодействия, направленного на предотвращение компьютерных атак на информационные ресурсы, в том числе на объекты критической информационной инфраструктуры.

4. Объекты защиты информационной безопасности

4.1. Объектами защиты информационной безопасности являются информация и информационные ресурсы ОИВ, обрабатываемые в информационных системах и их функциональных подсистемах, содержащие сведения, доступ к которым ограничен, и используемые в процессах сбора, обработки, накопления, хранения и распространения в рамках информационных систем ОИВ:

информационные ресурсы ОИВ ограниченного распространения, в том числе, содержащие конфиденциальные сведения;

программные информационные ресурсы ОИВ, в том числе, прикладное программное обеспечение, системное программное обеспечение, инструментальные средства и утилиты;

физические и информационные ресурсы ОИВ: компьютерное аппаратное обеспечение всех видов; носители информации всех видов (электронные, бумажные и так далее).

4.2. Доступность информации, целостность информации и конфиденциальность информации в обязательном порядке должны учитываться ОИВ при разработке организационно-распорядительной документации по обеспечению информационной безопасности для системы в целом и для каждого её ресурса в отдельности.

5. Принципы обеспечения информационной безопасности

5.1. Принципами обеспечения информационной безопасности являются:

внедрения СУИБ в ОИВ;

применение в ОИВ разнородных систем обеспечения информационной безопасности;

многоуровневость СУИБ;

расположение особо важных информационных ресурсов ОИВ в зоне максимальной безопасности;

непрерывность и целенаправленность процесса обеспечения в ОИВ ИБ;

усиление защиты информации в ОИВ во время нештатных ситуаций;

обеспечение возможности регулирования уровня ИБ в ОИВ без изменения функциональной базы СУИБ;

доступность применения механизмов защиты в ОИВ.

5.2. СУИБ включает в себя проведение организационных мероприятий в целях ИБ, а также кадровое и правовое обеспечение ИБ.

5.3. Проведение организационных мероприятий в целях ИБ:

составление реестра (перечня) ИС и АИС, подлежащего пересмотру не реже 1 раза в год, по следующей классификации:

содержащие информацию ограниченного доступа;

содержащие общедоступную информацию;

содержащие системы обработки и анализа информации, технические и программные средства её обработки, передачи и отображения, в том числе каналы информационного обмена и телекоммуникации, системы и средства защиты информации, объекты и помещения, в которых размещены такие системы;

оценка рисков информационной безопасности;

соблюдение правил физической защиты;

соблюдение правил внешнего доступа;

соблюдение правил работы в информационно-телекоммуникационной сети Интернет;

соблюдение правил безопасности электронной почты;

соблюдение правил управления доступом;

соблюдение правил работы со средствами криптографической защиты;

управление непрерывностью работы в ОИВ.

5.4. Кадровое и правовое обеспечение ИБ заключается в:

совершенствовании порядка формирования кадрового состава ОИВ, обеспечивающего эффективность информационной безопасности в ОИВ;

правовом сопровождении деятельности по обеспечению информационной безопасности в ОИВ.

6. Оценка рисков информационной безопасности

6.1. Для обеспечения бесперебойного функционирования оценка рисков информационной безопасности организуется и проводится лицами, ответственными за организацию и проведение работ по обеспечению информационной безопасности в ОИВ.

6.2. Оценка рисков производится экспертным методом на основании мнений оценок экспертов, включённых в комиссию, состав которой утверждается приказом ОИВ.

6.3. Результат оценки рисков учитывается в модели угроз информационной безопасности.

6.4. Оценка рисков при составлении и пересмотре организационно-распорядительных документов ОИВ проводится с учетом:

ущерба, который может нанести деятельности ОИВ в результате нарушений требований информационной безопасности, с учётом возможных последствий нарушений конфиденциальности, целостности и доступности информации;

реальной вероятности такого нарушения защиты.

7. Правила физической защиты

7.1. Установка и использование компьютерного аппаратного обеспечения должны осуществляется ответственными сотрудниками в ОИВ в соответствии с правилами установки и эксплуатации, установленными разработчиком (продавцом) компьютерного аппаратного обеспечения.

7.2. Перед проведением модернизации компьютерного аппаратного обеспечения или его ремонта, а также перед выполнением манипуляций с носителями информации необходимо выполнить резервное копирование данных.

7.3. После выполнения процесса модернизации аппаратного и (или) программного обеспечения необходимо провести внеплановое техническое обслуживание всей системы.

7.4. Техническое обслуживание компьютерного оборудования и программного обеспечения (физическая очистка оборудования, поддержание программного обеспечения в работоспособном состоянии), а также резервное копирование данных проводится регулярно,

не реже 1 раза в неделю с учётом рекомендаций разработчиков данного оборудования и(или) программного обеспечения.

7.5. После проведения резервного копирования данных необходимо проверить работоспособность и корректность полученной копии.

7.6. Резервному копированию в обязательном порядке подлежат:

все конфиденциальные данные в ИС, АС;

все исходные материалы для разработки собственного программного обеспечения и прочих проектов;

данные системы, без которых невозможна работа;

прочие данные, которые записаны на физически изнашиваемых носителях информации и носителях, поддерживающих операции перезаписи;

иные данные согласно решению уполномоченных сотрудников ОИВ.

7.7. Во время резервного копирования данных, а также во время записи любой информации на носители информации однократной записи, другие виды работ на той компьютерной системе, при помощи которой осуществляется эта запись не проводятся.

7.8. Все носители (электронные, бумажные) с конфиденциальной информацией и их резервные копии должны храниться в недоступном для посторонних, защищённом от света и других вредоносных внешних воздействий месте с соблюдением правил безопасного хранения для любого вида носителя информации.

7.9. Необходимо размещать системы вывода информации (мониторы, дисплеи) способом, исключающий видимость для посторонних лиц.

7.10. При возникновении аварийной ситуации необходимо прекратить эксплуатацию аварийного устройства, немедленно поставить в известность руководителя ОИВ или назначенное им лицо, ответственное за организацию и проведение работ по обеспечению информационной безопасности.

7.11. В случае списания носителей, содержащих конфиденциальную информацию (компьютерной техники, носителей информации) необходимо обеспечить полное и безвозвратное уничтожение содержащейся на ней конфиденциальной и любой другой информации после выполнения процедуры переноса основных информационных ресурсов со списываемого оборудования.

8. Правила внешнего доступа

8.1. Ответственным сотрудникам в ОИВ перед подключением к СУПД, необходимо принять комплекс мер, предусмотренных постановлением Губернатора Волгоградской области от 23 июня 2014 г. № 528 "О вопросах эксплуатации Сети управления и передачи данных Волгоградской области и локальных вычислительных сетей органов исполнительной власти Волгоградской области" по установлению защиты

от вредоносного воздействия в сети.

8.2. На АРМ должны быть обеспечены меры для предотвращения заражения вирусным программным обеспечением.

8.3. На АРМ с помощью соответствующего программного обеспечения (антивирус, брандмауэр) и настроек параметров его безопасности необходимо обеспечить контроль за входящей и исходящей информацией, а также за наличием вирусного программного обеспечения в потенциально опасных местах хранения информации.

8.4. АРМ должно подвергаться периодической проверке антивирусными средствами (не реже чем раз в месяц) и другими средствами, обеспечивающими безопасность. В случае обнаружения вирусного программного обеспечения при проведении антивирусной проверки сотрудники ОИВ обязаны:

приостановить работу на АРМ;

немедленно поставить в известность о факте обнаружения вирусного программного обеспечения своего непосредственного руководителя, владельца заражённых файлов, смежные структурные подразделения ОИВ, использующие эти файлы в работе, а также сотрудников отдела по обеспечению ИТ-инфраструктуры государственного бюджетного учреждения Волгоградской области "Центр информационных технологий Волгоградской области" любым доступным способом.

8.5. Перед использованием все внешние носители информации, полученные из любых источников, должны подвергаться полному антивирусному сканированию.

8.6. Версии программного обеспечения (включая обновления, связанные с управлением аппаратным обеспечением системы: драйверы устройств), а также те, которые связаны с работой с сетью и предназначены для обеспечения информационной безопасности, подлежат регулярному обновлению.

8.7. Зараженные данные подлежат немедленному удалению.

9. Правила работы в информационно-телекоммуникационной сети Интернет

9.1. При использовании сети Интернет необходимо:

соблюдать требования настоящего Регламента;

ставить в известность сотрудника, ответственного за обеспечение ИБ в ОИВ, о любых фактах нарушения требований настоящего Регламента.

9.2. При использовании сети Интернет запрещено:

использовать несанкционированные аппаратные и программные средства (мобильные телефоны, внешние модемы), позволяющие получить несанкционированный доступ к сети Интернет из СУПД;

совершать любые действия, направленные на нарушение функционирования ИС, АС.

9.3. Все файлы, полученные из информационно-

телекоммуникационной сети Интернет, перед их использованием в работе подлежат антивирусной проверке.

9.4. Комитет вправе производить отключение от СУПД пользователей СУПД, а также информационных сетей и ресурсов в случаях, если они препятствуют функционированию СУПД или представляют угрозу безопасности информации или техническим средствам СУПД.

10.Правила безопасности электронной почты

10.1. Все наиболее важные сообщения электронной почты должны архивироваться. Также регулярной архивации должна подвергаться информация, касающаяся данных о сотрудниках, с которыми осуществляется связь средствами электронной почты (адресные книги и т.п.).

10.2. Все ранее сохранённые почтовые сообщения, потерявшие свою актуальность, должны быть безвозвратно уничтожены со всех носителей информации.

10.3. Необходимо в обязательном порядке проверять каждое исходящее и получаемое сообщение электронной почты на наличие потенциально опасного содержимого. Почтовые сообщения, не удовлетворяющие установленным требованиям, должны немедленно и безвозвратно удаляться без прочтения.

10.4. На почтовом сервере устанавливаются, при необходимости, ограничения на содержимое и размер принимаемых сообщений. Сообщения, которые не удовлетворяют установленным критериям, должны сервером отклоняться.

10.5. После отправки письма по электронной почте необходимо хранить его до тех пор, пока не будет подтверждения доставки получателю.

10.6. Все файлы, полученные вместе с сообщением электронной почты без запроса со стороны владельца электронной почты, на которую получено сообщение, должны немедленно и безвозвратно удаляться без оценки их полезности.

10.7. В случае получения на электронную почту из любых источников сообщений, содержащих информацию сомнительного характера, запрещается:

переходить по ссылкам из электронных сообщений;

сообщать в ответном письме аутентификационные данные пользователя (логин и пароль).

10.8. Указанные сообщения передаются сотрудникам отдела по обеспечению ИТ-инфраструктуры государственного бюджетного учреждения Волгоградской области "Центр информационных технологий Волгоградской области" для анализа, а после этого — безвозвратно удаляются.

11.Правила управления доступом

11.1. Работы в ИС, АС осуществляют сотрудники ОИВ, после их регистрации и положительной аутентификации.

11.2. Регистрации подлежат все попытки входа в ИС, АС.

11.3. Руководитель ОИВ назначает лицо, ответственное за аудит доступа сотрудников ОИВ к их объектам.

11.4. Правила составления и использования к информационным ресурсам:

пароль должен состоять не менее чем из двенадцати символов, произвольных комбинаций букв верхнего и нижнего регистра, цифр и специальных символов;

все пароли подлежат изменению не реже, чем раз в три месяца, использовать пароли повторно запрещается;

использовать одинаковые пароли для доступа к разным информационным ресурсам запрещается;

пароли необходимо хранить в надёжном, недоступном для посторонних месте или же использовать специальные аппаратные средства для их хранения;

хранение паролей должно осуществляется операционной системой, установленный ею уровень защиты не может быть снижен;

сообщать пароли третьим лицам запрещается;

указывать пароли в общедоступных местах запрещается;

имена и пароли для доступа к каким-либо информационным ресурсам, которые не используются, подлежат блокировке;

система должна предотвращать попытки регистрации/перерегистрации тех сотрудников ОИВ, чьи имена и пароли входа в систему не соответствуют установленным правилам;

при получении доступа к информационному ресурсу при помощи процедуры авторизации по имени и паролю разглашать их запрещается;

пароли подлежат замене в случае возникновения возможности их компрометации;

при увольнении сотрудника ОИВ необходимо незамедлительно осуществить блокировку его учётных данных во всех информационных ресурсах.

12. Правила работы со средствами криптографической защиты

12.1. Все поступающие средства криптографической защиты информации (далее – СКЗИ) должны быть учтены в соответствующем журнале поэкземплярного учёта СКЗИ.

12.2. Эксплуатация средств криптографической защиты информации (СКЗИ) осуществляется в соответствии с:

нормативными правовыми актами и методическими документами уполномоченного органа в сфере криптографической защиты информации;

эксплуатационной документацией завода-изготовителя (руководством по эксплуатации, формуляром, паспортом, техническим описанием);

внутренними организационно-распорядительными документами ОИВ, регламентирующими порядок применения СКЗИ.

12.3. В целях эффективного применения криптографических методов осуществляется управление криптографическими ключами.

12.4. Все криптографические ключи должны быть защищены от изменения, утери и уничтожения, а также от несанкционированного раскрытия. Оборудование, используемое для генерации, хранения и архивирования криптографических ключей, должно быть физически защищено.

12.5. При использовании шифрования в ГИС, ИС и АС должны применяться только утверждённые стандартные алгоритмы и сертифицированные в установленном порядке продукты, их реализующие.

13. Управление непрерывностью работы в ОИВ

13.1. В целях противодействия прерыванию работы в ОИВ и защиты рабочих процессов от последствий при значительных сбоях или действиях осуществляется управление непрерывностью работы, путем:

анализа последствий от нарушений безопасности и отказов в обслуживании;

утверждение руководителем ОИВ плана непрерывности рабочего процесса в соответствии с согласованными целями и приоритетами;

утверждение руководителем ОИВ стратегии определения общего подхода к обеспечению непрерывности работы.

13.2. Планирование непрерывности работы включает:

идентификации событий, которые могут быть причиной прерывания работы (например отказ оборудования, наводнение, пожар);

оценку рисков с целью определения последствий этих прерываний (с точки зрения масштаба повреждения, а также периода восстановления);

13.3. План обеспечения непрерывности работы должен содержать следующие мероприятия по обеспечению информационной безопасности:

определение и согласование всех обязанностей должностных лиц ОИВ и процедур на случай чрезвычайных ситуаций;

внедрение в случае чрезвычайных ситуаций процедур, обеспечивающих возможность восстановления рабочего процесса в течение требуемого времени;

оценку зависимости работы от внешних факторов и существующих контрактов;

документирование согласованных процедур и процессов;

обучение сотрудников ОИВ действиям при возникновении чрезвычайных ситуаций, включая кризисное управление.

14. Заключительные положения

Ответственность за организацию и проведение работ по обеспечению информационной безопасности в ОИВ несёт руководитель ОИВ или назначенное им лицо.

При возникновении проблем с безопасностью ИС, АС (например, при успешном взломе системы безопасности) возникшая проблема должна быть немедленно проанализирована, а организационно-распорядительные документы ОИВ по информационной безопасности пересмотрены в соответствии с проведённым анализом.