



ПРАВИТЕЛЬСТВО ВОЛОГОДСКОЙ ОБЛАСТИ

ПОСТАНОВЛЕНИЕ

От 09.07.2025

г. Вологда

№ 990

Об осуществлении полномочий исполнительных органов области по обеспечению информационной безопасности

В соответствии с Указом Президента Российской Федерации от 1 мая 2022 года № 250 «О дополнительных мерах по обеспечению информационной безопасности Российской Федерации», постановлением Правительства Российской Федерации от 15 июля 2022 года № 1272 «Об утверждении типового положения о заместителе руководителя органа (организации), ответственном за обеспечение информационной безопасности в органе (организации), и типового положения о структурном подразделении в органе (организации), обеспечивающем информационную безопасность органа (организации)»

Правительство области **ПОСТАНОВЛЯЕТ:**

1. Определить Министерство цифрового развития области органом, реализующим задачи и осуществляющим функции по обеспечению информационной безопасности Правительства области и исполнительных органов области согласно приложению к настоящему постановлению.

2. Внести в Положение о Министерстве цифрового развития Вологодской области, утвержденное постановлением Правительства области от 8 ноября 2024 года № 1310, следующие изменения:

2.1. Пункт 3.1.16 изложить в следующей редакции:

«3.1.16. Координирует выполнение мероприятий по созданию, развитию, эксплуатации и выводу из эксплуатации информационных систем и региональной информационно-телекоммуникационной инфраструктуры исполнительными органами области, включая вопросы обеспечения информационной безопасности.».».

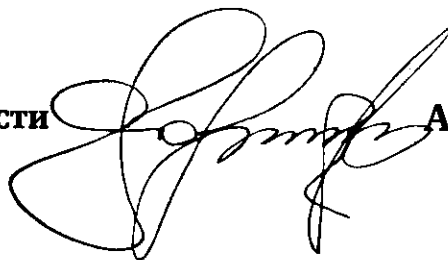
2.2. Пункт 3.2 дополнить подпунктом 3.2.36 следующего содержания:

«3.2.36. Осуществляет функции органа по обеспечению информационной безопасности Правительства области и исполнительных органов области в соответствии с постановлением Правительства области от 9 июля 2025 года № 990 «Об осуществлении полномочий исполнительных органов области по обеспечению информационной безопасности».».

3. Министерству цифрового развития области представить изменения в Положение о Министерстве цифрового развития Вологодской области в Управление Федеральной налоговой службы по Вологодской области для государственной регистрации.

4. Настоящее постановление вступает в силу со дня его официального опубликования.

Председатель Правительства области



А.М. Мордвинов

Задачи и функции органа, обеспечивающего информационную безопасность Правительства области и исполнительных органов области

1. Деятельность органа, обеспечивающего информационную безопасность, направлена на:

- а) исключение или существенное снижение негативных последствий (ущерба) в отношении Правительства области и исполнительных органов области (далее – исполнительные органы области) вследствие нарушения функционирования информационных систем, информационно-телекоммуникационных сетей и автоматизированных систем управления в результате реализации угроз безопасности информации;
- б) обеспечение конфиденциальности информации, доступ к которой ограничен в соответствии с законодательством Российской Федерации;
- в) повышение защищенности исполнительных органов области от возможного нанесения им материального, репутационного или иного ущерба посредством случайного или преднамеренного несанкционированного вмешательства в процесс функционирования информационных систем исполнительных органов области или несанкционированного доступа к циркулирующей в них информации и ее несанкционированного использования;
- г) обеспечение надежности и эффективности функционирования и безопасности информационных систем, производственных процессов и информационно-технологической инфраструктуры исполнительных органов области;
- д) обеспечение выполнения требований по информационной безопасности при создании и функционировании информационных систем и информационно-телекоммуникационной инфраструктуры исполнительных органов области.

2. Основными задачами деятельности органа, обеспечивающего информационную безопасность, являются:

- а) планирование, организация и координация работ по обеспечению информационной безопасности и контроль за ее состоянием в исполнительных органах области;
- б) выявление угроз безопасности информации и уязвимостей информационных систем, программного обеспечения и программно-аппаратных средств;
- в) предотвращение утечки информации по техническим каналам, несанкционированного доступа к ней, специальных воздействий на информацию (носители информации) в целях ее добывания, уничтожения, искажения и блокирования доступа к ней;
- г) поддержание стабильной деятельности исполнительных органов области в случае проведения компьютерных атак;
- д) взаимодействие с Национальным координационным центром по компьютерным инцидентам;

е) обеспечение нормативно-правового обеспечения использования информационных ресурсов.

3. Орган, обеспечивающий информационную безопасность, выполняет следующие функции:

а) разработка, координация, управление и контроль за реализацией плана (программы) работ по обеспечению информационной безопасности в исполнительных органах области;

б) разработка предложений по совершенствованию организационно-распорядительных документов по обеспечению информационной безопасности в исполнительных органах области;

в) выявление и проведение анализа угроз безопасности информации в отношении исполнительных органов области, уязвимостей информационных систем, программного обеспечения программно-аппаратных средств и принятие мер по их устранению;

г) обеспечение в соответствии с требованиями по информационной безопасности, в том числе с целью исключения (невозможности реализации) негативных последствий, разработки и реализации организационных мер и применения средств обеспечения информационной безопасности;

д) обнаружение, предупреждение и ликвидация последствий компьютерных атак и реагирование на компьютерные инциденты;

е) представление в Национальный координационный центр по компьютерным инцидентам информации о выявленных компьютерных инцидентах;

ж) исполнение указаний, данных Федеральной службой безопасности Российской Федерации и ее территориальными органами, Федеральной службой по техническому и экспортному контролю по результатам мониторинга защищенности информационных ресурсов, принадлежащих исполнительным органам области либо используемых ими, доступ к которым обеспечивается посредством использования информационно-телекоммуникационной сети «Интернет»;

з) проведение анализа и контроля за состоянием защищенности систем и сетей и разработка предложений по модернизации (трансформации) основных процессов исполнительных органов области в целях обеспечения информационной безопасности;

и) подготовка отчетов о состоянии работ по обеспечению информационной безопасности в исполнительных органах области;

к) организация развития навыков безопасного поведения в исполнительных органах области, в том числе проведение занятий с руководящим составом и специалистами по вопросам обеспечения информационной безопасности;

л) выполнение иных функций исходя из поставленных Губернатором области и Правительством области целей и задач в рамках обеспечения информационной безопасности в исполнительных органах области.

С целью реализации функций орган, обеспечивающий информационную безопасность, имеет право:

а) запрашивать и получать в установленном порядке доступ к работам и документам исполнительных органов области, необходимым для принятия решений по всем вопросам, отнесенным к компетенции органа, обеспечивающего информационную безопасность;

б) готовить предложения о привлечении к проведению работ по обеспечению информационной безопасности организаций, имеющих лицензии на соответствующий вид деятельности;

в) контролировать деятельность исполнительных органов области по выполнению требований к обеспечению информационной безопасности;

г) постоянно повышать профессиональные компетенции, знания и навыки работников в области обеспечения информационной безопасности;

д) участвовать в пределах своей компетенции в отраслевых, межотраслевых, межрегиональных и международных выставках, семинарах, конференциях, в работе межведомственных рабочих групп, отраслевых экспертных сообществ, международных органов и организаций;

е) участвовать в работе коллегиальных органов при рассмотрении вопросов обеспечения информационной безопасности;

ж) вносить предложения Губернатору области, Правительству области, руководителям исполнительных органов области о приостановлении работ в случае обнаружения факта нарушения информационной безопасности;

з) вносить представления Губернатору области, Правительству области, руководителям исполнительных органов области в отношении государственных гражданских служащих при обнаружении фактов нарушения ими установленных требований безопасности информации, в том числе ходатайствовать о привлечении их к ответственности.