МИНИСТЕРСТВО АРХИТЕКТУРЫ И СТРОИТЕЛЬСТВА СМОЛЕНСКОЙ ОБЛАСТИ

П Р И К А З

«01» 07 2025 № 119-ОД

О структурном подразделении Министерства архитектуры и строительства Смоленской области, осуществляющем функции по обеспечению информационной безопасности

В целях выполнения требований Указа Президента Российской Федерации от 1 мая 2022 г. № 250 «О дополнительных мерах по обеспечению информационной безопасности Российской Федерации»,

п р и к а з ы в а ю :

1. Возложить на структурное подразделение «Отдел цифровизации и информационных систем» ответственность по обеспечению информационной безопасности Министерства архитектуры и строительства Смоленской области, в том числе по:

– обнаружению, предупреждению и ликвидации последствий компьютерных атак и реагированию на компьютерные инциденты.

2. Утвердить прилагаемое Положение о структурном подразделении Министерства архитектуры и строительства Смоленской области, обеспечивающем информационную безопасность.

3. Контроль за исполнением настоящего приказа оставляю за собой.

Министр К.Н. Ростовцев

УТВЕРЖДЕНО
приказом Министерства
архитектуры и строительства
Смоленской области
от «01» 07 2025 г. № 119-ОД

Положение о структурном подразделении Министерства архитектуры и строительства Смоленской области, обеспечивающем информационную безопасность

1. Общие положения

1.1. Настоящее положение определяет цели, задачи и функции структурного подразделения Министерства архитектуры и строительства Смоленской области (далее – Министерство), обеспечивающего информационную безопасность Министерства (далее – Подразделение).

1.2. Подразделение в своей деятельности руководствуется Конституцией Российской Федерации, федеральными конституционными законами, федеральными законами, актами Президента Российской Федерации и Правительства Российской Федерации, международными договорами Российской Федерации, нормативными правовыми и актами федеральных органов исполнительной власти, уполномоченных в области обеспечения информационной безопасности, другими нормативными правовыми документами в сфере обеспечения информационной безопасности, указаниями руководства Министерства, настоящим положением и иными локальными актами Министерства.

1.3. Подразделение подчиняется сотруднику Министерства, ответственному за обеспечение информационной безопасности в Министерстве архитектуры и строительства Смоленской области.

1.4. Контроль за деятельностью Подразделения осуществляет министр архитектуры и строительства Смоленской области.

2. Цели и задачи деятельности подразделения

2.1. Деятельность Подразделения направлена на:

– исключение или существенное снижение негативных последствий (ущерба) в отношении Министерства вследствие нарушения функционирования информационных систем, информационно-телекоммуникационных сетей и автоматизированных систем управления (далее – системы и сети) в результате реализации угроз безопасности информации.

– обеспечение конфиденциальности информации, доступ к которой ограничен в соответствии с законодательством Российской Федерации.

– повышение защищенности Министерства от возможного нанесения Министерству материального, репутационного или иного ущерба посредством случайного или преднамеренного несанкционированного вмешательства в процесс функционирования систем и сетей Министерства или несанкционированного доступа к циркулирующей в них информации и ее несанкционированного использования.

– обеспечение надежности и эффективности функционирования и безопасности систем и сетей, производственных процессов и информационно-технологической инфраструктуры Министерства.

– обеспечение выполнения требований по информационной безопасности при создании и функционировании систем и сетей и информационно-телекоммуникационной инфраструктуры Министерства.

2.2. Основными задачами деятельности Подразделения являются:

– планирование, организация и координация работ по обеспечению информационной безопасности и контроль за ее состоянием в Министерстве.

– выявление угроз безопасности информации и уязвимостей систем и сетей, программного обеспечения и программно-аппаратных средств.

– 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.

– поддержание стабильной деятельности Министерства и производственных процессов Министерства в случае проведения компьютерных атак.

– взаимодействие с Национальным координационным центром по компьютерным инцидентам.

– обеспечение нормативно-правового обеспечения использования информационных ресурсов.

3. Функции подразделения

3.1. Подразделение выполняет следующие функции:

3.1.1 Разработка, координация, управление и контроль за реализацией плана (программы) работ по обеспечению информационной безопасности в Министерстве;

3.1.2 Разработка предложений по совершенствованию организационно-распорядительных документов по обеспечению информационной безопасности в Министерстве и представление их министру архитектуры и строительства Смоленской области или сотруднику Министерства, ответственному за обеспечение информационной безопасности в Министерстве архитектуры и строительства Смоленской области;

3.1.3 Выявление и проведение анализа угроз безопасности информации в отношении Министерства, уязвимостей систем и сетей, программного обеспечения программно-аппаратных средств и принятие мер по их устранению;

3.1.4 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;

3.1.5 Обнаружение, предупреждение и ликвидация последствий компьютерных атак и реагирование на компьютерные инциденты;

3.1.6 Представление в Национальный координационный центр по компьютерным инцидентам информации о выявленных компьютерных инцидентах;

3.1.7 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 Министерству либо используемых Министерством, доступ к которым обеспечивается посредством использования информационно-телекоммуникационной сети «Интернет»;

3.1.8 Проведение анализа и контроля за состоянием защищенности систем и сетей и разработка предложений по модернизации (трансформации) основных процессов Министерства в целях обеспечения информационной безопасности в Министерстве;

3.1.9 Подготовка отчетов о состоянии работ по обеспечению информационной безопасности в Министерстве;

3.1.10 Организация развития навыков безопасного поведения в Министерстве, в том числе проведение занятий с руководящим составом и сотрудниками Министерства по вопросам обеспечения информационной безопасности;

3.1.11 Взаимодействие с сотрудниками Министерства, ответственными за обеспечение безопасности персональных данных и за защиту информации в информационных системах при решении вопросов, связанных с созданием системы защиты информации информационных систем, их эксплуатацией и выводом из эксплуатации.

3.1.12 Выполнение иных функций, исходя из поставленных руководством Министерства целей и задач в рамках обеспечения информационной безопасности в Министерстве.

4. Права подразделения

4.1. С целью реализации функций Подразделение имеет право:

– знакомиться с локальными актами Министерства, регламентирующими процессы обработки информации;

– запрашивать и получать в установленном порядке доступ к работам и документам структурных подразделений Министерства, необходимым для принятия решений по всем вопросам, отнесенным к компетенции Подразделения;

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

– контролировать деятельность любого структурного подразделения Министерства по выполнению требований к обеспечению информационной безопасности;

– постоянно повышать профессиональные компетенции, знания и навыки сотрудников в области обеспечения информационной безопасности;

– 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;

– участвовать в работе комиссий Министерства при рассмотрении вопросов обеспечения информационной безопасности;

– вносить предложения руководству Министерства о приостановлении работ в случае обнаружения факта нарушения информационной безопасности;

– вносить представления руководству Министерства в отношении сотрудников Министерства при обнаружении фактов нарушения сотрудниками установленных требований безопасности информации в Министерстве, в том числе ходатайствовать о привлечении указанных сотрудников к административной или уголовной ответственности;

– вносить на рассмотрение руководству Министерства предложения по вопросам деятельности Подразделения;

– обращаться за необходимыми разъяснениями по вопросам обработки персональных данных к ответственному за организацию обработки персональных данных.

5. Взаимоотношения и связи подразделения

5.1. Подразделение осуществляет свои полномочия во взаимодействии со структурными подразделениями Министерства, а также в пределах своей компетенции с иными органами (организациями) и гражданами в установленном порядке.

5.2. По указанию руководства Министерства осуществляет взаимодействие с Федеральной службой безопасности Российской Федерации, Федеральной службой по техническому и экспортному контролю и Министерством цифрового развития,

связи и массовых коммуникаций Российской Федерации по вопросам информационной безопасности.

6. Показатели эффективности и результативности подразделения

6.1. Эффективность и результативность деятельности Подразделения определяются по итогам выполнения Министерством программы обеспечения информационной безопасности.

7. Ответственность

7.1. Сотрудники Подразделения несут ответственность за:

– ненадлежащее выполнение возложенных на них обязанностей в соответствии с утвержденными должностными регламентами и настоящим Положением.

– разглашение информации в пределах, установленных действующим административным, уголовным и гражданским законодательством Российской Федерации.

– несоблюдение требований локальных актов Министерства по обеспечению информационной безопасности, в пределах, установленных трудовым договором (служебным контрактом).