Приложение № 2

Утверждено
приказом департамента
агропромышленного комплекса
Костромской области
от 31.01 2022 года № 18

Положение
об обработке и защите конфиденциальной информации в автоматизированных информационных системах департамента агропромышленного комплекса Костромской области

Глава 1. ОБЩИЕ ПОЛОЖЕНИЯ

1. Настоящее Положение об обработке и защите конфиденциальной информации в автоматизированных информационных системах департамента агропромышленного комплекса Костромской области (далее - Департамент) разработано в соответствии с Федеральным законом от 27 июля 2006 года № 149-ФЗ «Об информации, информационных технологиях и о защите информации», Федеральным законом от 27 июля 2006 года № 152-ФЗ «О персональных данных», «Специальными требованиями и рекомендациями по технической защите конфиденциальной информации (СТР-К)», утвержденными Приказом Государственной технической комиссии Российской Федерации от 30 августа 2002 года № 282, национальным стандартом Российской Федерации «Защита информации. Основные термины и определения. ГОСТ Р 50922-2006», утвержденным Приказом Федерального агентства по техническому регулированию и метрологии от 27 декабря 2006 года № 373-ст, Приказами Федеральной службы по техническому и экспортному контролю Российской Федерации от 11 февраля 2013 года № 17 «Об утверждении Требований о защите информации, не составляющей государственную тайну, содержащейся в государственных информационных системах», от 18 февраля 2013 года № 21 «Об утверждении Состава и содержания организационных и технических мер по обеспечению безопасности персональных данных при их обработке в информационных системах персональных данных».

2. Настоящее Положение определяет цели обработки и защиты конфиденциальной информации, объекты защиты конфиденциальной информации, организационную систему обработки и защиты конфиденциальной информации, в том числе персональных данных в автоматизированных информационных системах Департамента, основные направления и методы защиты конфиденциальной информации в автоматизированных информационных системах Департамента, обязанности и ответственность пользователей и должностных лиц при обработке конфиденциальной информации в автоматизированных информационных системах Департамента, а также ответственность за разглашение конфиденциальной информации.

3. Настоящее Положение не распространяется на вопросы защиты информации, содержащей государственную тайну.

4. В Положении используются термины и определения, установленные в актах, указанных в пункте 1 настоящего Положения.

Глава 2. ЦЕЛИ ОБРАБОТКИ И ЗАЩИТЫ КОНФИДЕНЦИАЛЬНОЙ ИНФОРМАЦИИ

5. Основной целью обработки конфиденциальной информации в автоматизированных информационных системах Департамента является повышение эффективности исполнения Департаментом установленных законодательством полномочий.

6. Основными целями защиты конфиденциальной информации в автоматизированных информационных системах Департамента являются:

1) предотвращение неконтролируемого распространения конфиденциальной информации в результате ее разглашения сотрудниками или получения несанкционированного доступа к информации;

2) предотвращение несанкционированного уничтожения, искажения, копирования, блокирования информации;

3) предотвращение утрат, несанкционированного уничтожения или сбоев функционирования машинных носителей информации, обеспечение полноты, целостности, достоверности информации;

4) соблюдение правового режима использования автоматизированных информационных систем Департамента;

5) обеспечение возможности обработки и использования конфиденциальной информации сотрудниками Департамента, имеющими соответствующие полномочия.

Глава 3. ОБЪЕКТЫ ЗАЩИТЫ КОНФИДЕНЦИАЛЬНОЙ ИНФОРМАЦИИ

7. Объектами защиты конфиденциальной информации в информационных системах Департамента являются: информация, ее материальные носители, программные и технические средства обработки, передачи и защиты информации (далее - Активы).

8. Защите подлежат следующие Активы:

1) информационные ресурсы, содержащие сведения, отнесенные к категории информации конфиденциального характера, представленные в виде отдельных документов, информационных массивов и баз данных, зафиксированных на машинных носителях;

2) основные технические средства и системы информатизации (средства вычислительной техники, информационно-вычислительные комплексы, сети и системы), программные средства (операционные системы, системы управления базами данных, другое общесистемное и программное обеспечение), телекоммуникационные системы, используемые для обработки и передачи информации, содержащей сведения, отнесенные к конфиденциальной информации;

3) вспомогательные технические средства и системы, не обрабатывающие информацию, но размещенные в помещениях, где обрабатывается информация, содержащая сведения, отнесенные к конфиденциальной информации.

Глава 4. ОРГАНИЗАЦИОННАЯ СИСТЕМА ОБРАБОТКИ И ЗАЩИТЫ КОНФИДЕНЦИАЛЬНОЙ ИНФОРМАЦИИ

9. Организационную систему обработки и защиты конфиденциальной информации в автоматизированных информационных системах Департамента образуют:

1) директор департамента - осуществляет общее руководство по вопросам обработки и защиты конфиденциальной информации в автоматизированных информационных системах Департамента;

2) заместитель директора Департамента, курирующий вопросы по защите информации, - осуществляет распорядительные функции по организации работ по обработке и защите конфиденциальной информации в автоматизированных информационных системах Департамента, взаимодействует с надзорными органами по общим вопросам обработки и защиты конфиденциальной информации в Департаменте;

3) администратор информационной безопасности по обработке персональных данных на объектах информатизации Департамента – осуществляет работу по защите конфиденциальной информации в автоматизированных информационных системах Департамента;

3) руководители структурных подразделений Департамента, в которых производится обработка конфиденциальной информации - организуют обработку конфиденциальной информации в своем структурном подразделении;

4) отдел организационной работы и информационных технологий Департамента - организует работу по технической защите конфиденциальной информации в автоматизированных информационных системах Департамента, производит оценку эффективности применяемых мер технической защиты конфиденциальной информации в автоматизированных информационных системах Департамента;

5) пользователи (потребители) информации (далее - Пользователи) - сотрудники структурных подразделений Департамента, наделенные соответствующими правами по доступу к конфиденциальной информации и непосредственно использующие эту информацию для исполнения своих должностных обязанностей или выполняющие непосредственные действия по вводу, хранению, обработке и передаче конфиденциальной информации;

6) технические специалисты - сотрудники сторонних организаций, привлекаемые к работам в Департаменте на основании договоров, осуществляющие технические действия по эксплуатации средств вычислительной техники и автоматизированных информационных систем Департамента.

10. Для проведения работ по защите конфиденциальной информации в автоматизированных информационных системах Департамента могут привлекаться на договорной основе специализированные организации, имеющие соответствующие лицензии на право проведения работ в области защиты информации.

Глава 5. ОСНОВНЫЕ НАПРАВЛЕНИЯ И МЕТОДЫ ЗАЩИТЫ КОНФИДЕНЦИАЛЬНОЙ ИНФОРМАЦИИ

11. Основными направлениями работ по защите конфиденциальной информации являются:

1) физическая защита помещений, в которых обрабатывается конфиденциальная информация, от проникновения посторонних лиц;

2) физическая защита Активов от хищения, разрушения, уничтожения;

3) защита от несанкционированного доступа к конфиденциальной информации, несанкционированного или непреднамеренного воздействия;

4) защита от преднамеренных или непреднамеренных действий Пользователей, ведущих к утечке или утрате конфиденциальной информации.

12. Мероприятия по защите конфиденциальной информации включают в себя организационно-распорядительные, технические и контрольно-корректирующие.

13. Организационно-распорядительные мероприятия по защите конфиденциальной информации включают в себя:

1) разработку организационно-распорядительных документов по защите конфиденциальной информации;

2) ограничение числа лиц, допущенных к обработке конфиденциальной информации;

3) организацию контролируемой зоны, размещение объекта защиты внутри контролируемой зоны на максимально возможном удалении от ее границ, ограничение доступа лиц, не допущенных к обработке конфиденциальной информации, внутрь контролируемой зоны;

4) размещение дисплеев и других средств отображения, исключающее несанкционированный просмотр информации;

5) документальное оформление перечня сведений конфиденциального характера, Реестра автоматизированных информационных систем Департамента, обрабатывающих конфиденциальную информацию;

6) инвентаризацию, учет и надежное хранение Активов, содержащих конфиденциальную информацию или посредством которых производится обработка конфиденциальной информации;

7) классификацию и категорирование автоматизированных информационных систем Департамента, обрабатывающих конфиденциальную информацию исходя из требований законодательства и критичности для обеспечения государственного управления, в необходимых случаях - аттестацию автоматизированных информационных систем Департамента;

8) выявление угроз несанкционированного доступа к конфиденциальной информации, разработку мероприятий по нейтрализации угроз;

9) организацию и соблюдение правил парольной защиты в автоматизированных информационных системах Департамента;

10) повышение квалификации, совершенствование знаний и навыков Пользователей в вопросах защиты конфиденциальной информации;

11) дисциплинарную практику.

14. Мероприятия по технической защите информации включают в себя:

1) организацию физической защиты помещений и технических средств обработки информации с использованием организационных мер и технических

средств охраны, предотвращающих или существенно затрудняющих проникновение в здания, помещения посторонних лиц, хищение документов и носителей информации, самих средств информатизации;

2) сегментацию локальных вычислительных сетей в Департаменте, применение в сегментах локальных вычислительных сетей, в которых обрабатывается конфиденциальная информация, технических средств защиты информации, соответствующих требуемому классу защиты;

3) техническую реализацию системы парольной защиты для автоматизированных информационных систем Департамента, в которой обрабатывается конфиденциальная информация;

4) использование сертифицированных средств защиты информации в автоматизированных информационных системах Департамента при передаче информации по открытым каналам связи в соответствии с установленными законодательством требованиями;

5) регистрацию действий Пользователей, технических специалистов, контроль несанкционированного доступа и действий Пользователей, технических специалистов и посторонних лиц;

6) использование защищенных каналов связи, реализацию технологии частных виртуальных сетей в корпоративной вычислительной сети Департамента;

7) реализацию мероприятий по антивирусной защите в автоматизированных информационных системах Департамента;

8) реализацию системы резервного копирования информации.

15. Контрольно-корректирующие мероприятия по защите конфиденциальной информации включают в себя:

1) контроль исполнения законодательства в области защиты конфиденциальной информации;

2) контроль исполнения организационно-распорядительных документов;

3) контроль выполнения мероприятий по технической защите информации, оценку эффективности выполнения мероприятий по технической защите информации;

4) выработку корректирующих воздействий, реализуемых путем издания и последующего исполнения организационно-распорядительных документов;

5) применение дисциплинарных мер.

16. Порядок действий по реализации мероприятий по защите конфиденциальной информации определяется инструкциями и регламентами, разрабатываемыми и утверждаемыми в соответствии с принятым в Департаменте порядком.

Глава 6. ОБЯЗАННОСТИ И ОТВЕТСТВЕННОСТЬ ПРИ ОБРАБОТКЕ И ЗАЩИТЕ КОНФИДЕНЦИАЛЬНОЙ ИНФОРМАЦИИ В АВТОМАТИЗИРОВАННЫХ ИНФОРМАЦИОННЫХ СИСТЕМАХ ДЕПАРТАМЕНТА

17. Директор Департамента утверждает организационно-распорядительные документы по защите информации. Заместитель директора Департамента, курирующий вопросы по защите информации, осуществляет

контроль за организацией работы по обработке и защите информации в автоматизированных информационных системах Департамента.

18. Руководители структурных подразделений, в которых производится обработка конфиденциальной информации:

1) несут ответственность за организацию обработки конфиденциальной информации в своем структурном подразделении;

2) вносят предложения по включению в Реестр автоматизированных информационных систем обработки конфиденциальной информации Департамента, изменению или исключению соответствующих сведений в реестре;

3) вносят предложения и изменения в списки сотрудников, допускаемых к работе с конфиденциальной информацией, в эксплуатируемых автоматизированных информационных системах Департамента;

4) обеспечивают выполнение организационных мероприятий по обеспечению защиты конфиденциальной информации;

5) несут ответственность за соблюдение требований по защите конфиденциальной информации пользователями своих структурных подразделений и принимают меры по фактам нарушений требований по защите конфиденциальной информации, разглашения конфиденциальной информации или утери документов, содержащих такую информацию;

6) несут ответственность за своевременное информирование администратора информационной безопасности о необходимости уничтожения конфиденциальной информации с жестких дисков персональных компьютеров, передаваемых в ремонт или в другие структурные подразделения;

7) несут ответственность за выполнение Пользователями своего структурного подразделения общих правил работы на персональных компьютерах и в локальных вычислительных сетях Департамента, при передаче информации по каналам связи с использованием сертифицированных средств криптографической защиты информации, при организации доступа в информационно-телекоммуникационную сеть «Интернет», соблюдение Пользователями условий хранения средств технической защиты информации;

8) определяют порядок передачи информации конфиденциального характера другим структурным подразделениям Департамента, исполнительным органам государственной власти Костромской области, муниципальным образованиям Костромской области и сторонним организациям;

9) несут ответственность за характер исходящей информации, направляемой пользователями по электронной почте другим адресатам, и принятие оперативных мер к соблюдению установленных требований по защите конфиденциальной информации.

19. Отдел организационной работы и информационных технологий Департамента:

1) организует ведение реестра автоматизированных информационных систем Департамента, в которых осуществляется обработка конфиденциальной информации;

2) организует и обеспечивает исполнение работ по технической защите конфиденциальной информации в автоматизированных информационных системах Департамента;

3) осуществляет контроль состояния защиты конфиденциальной информации и производит оценку эффективности применяемых мер технической защиты информации в автоматизированных информационных системах Департамента;

4) осуществляет разработку проектов планов мероприятий по организации системы защиты информации в автоматизированных информационных системах Департамента, участвует в их исполнении;

5) представляет отчеты о состоянии системы защиты информации в автоматизированных информационных системах Департамента;

6) разрабатывает проекты организационно-распорядительных документов по вопросам обработки и технической защиты конфиденциальной информации в автоматизированных информационных Департамента;

7) разрабатывает предложения по совершенствованию системы защиты информации в Департамента.

20. Пользователи:

1) участвуют в обработке конфиденциальной информации, осуществляют непосредственные действия по регистрации информации в автоматизированных информационных Департамента, ее обработке, передаче по сетям передачи данных, применению сертифицированных средств защиты информации;

2) используют информацию, документы, полученные из автоматизированных информационных систем Департамента, в своей работе с целью реализации возложенных на них функций;

3) применяют (в необходимых случаях) сертифицированные средства защиты информации;

4) несут персональную ответственность за передачу или утерю носителей конфиденциальной информации, а также средств защиты информации.

Глава 7. ОТВЕТСТВЕННОСТЬ ЗА РАЗГЛАШЕНИЕ КОНФИДЕНЦИАЛЬНОЙ ИНФОРМАЦИИ

21. За разглашение информации конфиденциального характера, нарушение порядка обращения с документами и машинными носителями информации, содержащими такую информацию, а также за нарушение или неисполнение требований режима защиты, обработки и порядка использования этой информации сотрудник может быть привлечен к дисциплинарной, гражданско-правовой, административной или уголовной ответственности, предусмотренной действующим законодательством Российской Федерации.