

Платонов Константин Игоревич,
курсант 223 учебной группы, 2 факультета,
Филиал ВУНЦ ВВС «ВВА», Рф Г. Челябинск

Попов Юрий Леонидович,
К. И. Н., доцент, профессор АВН,
Филиал ВУНЦ ВВС «ВВА», Рф Г. Челябинск

ОРГАНИЗАЦИЯ СЕКРЕТНОСТИ В КОММЕРЧЕСКИХ ОРГАНИЗАЦИЯХ, ВЫПОЛНЯЮЩИХ ГОСУДАРСТВЕННЫЕ ЗАКАЗЫ

Аннотация: В статье рассматриваются особенности организации режима секретности в коммерческих организациях, выполняющих государственные заказы, включая работы и услуги, связанные с использованием сведений, составляющих государственную тайну. Анализируются нормативно-правовые акты, регламентирующие требования к защите информации, порядок получения допуска к государственной тайне, а также создание и функционирование подразделений по защите информации.

Ключевые слова: государственная тайна, секретность, режим секретности, контроль доступа, гриф секретности, защита информации.

Основным нормативным актом, регулирующим вопросы государственной тайны в Российской Федерации, является Закон РФ от 21 июля 1993 года № 5485-1 «О государственной тайне». Он определяет перечень сведений, подлежащих засекречиванию, устанавливает уровни секретности и порядок допуска к таким сведениям. Согласно статье 8 данного закона, уровень секретности информации должен соответствовать степени тяжести ущерба, который может быть нанесён безопасности государства вследствие её распространения. Существуют три уровня секретности: «особой важности», «совершенно секретно» и «секретно».

Федеральный закон от 29 июля 2004 года № 98-ФЗ «О коммерческой тайне» регулирует отношения, связанные с отнесением информации к коммерческой тайне, передачей такой информации и охраной её конфиденциальности. Закон определяет меры по охране конфиденциальности информации, включая установление перечня информации, ограничение доступа, учёт лиц, получивших доступ, и нанесение грифа «Коммерческая тайна» на соответствующие документы.

Трудовой кодекс Российской Федерации предоставляет работодателю право на установление требований к соблюдению режима коммерческой тайны. В трудовом договоре могут содержаться условия о неразглашении работником сведений, составляющих коммерческую тайну работодателя. Уголовный кодекс Российской Федерации предусматривает ответственность за незаконное получение и разглашение сведений, составляющих коммерческую, налоговую или банковскую тайну.

Коммерческая организация, привлекаемая к выполнению государственного заказа, должна разработать и утвердить внутренние нормативные документы, регулирующие порядок работы с конфиденциальной информацией. К таким документам относятся: Положение о защите государственной тайны; Положение о коммерческой тайне; Инструкции по обеспечению режима секретности; Должностные инструкции сотрудников, допущенных к работе с секретной информацией.

Для эффективного функционирования системы защиты информации необходимо назначить ответственных лиц за обеспечение режима секретности. В обязанности таких лиц



входит: контроль за соблюдением требований законодательства о государственной и коммерческой тайне; организация обучения персонала; проведение внутренних проверок и аудитов; взаимодействие с органами государственной власти.

Все сотрудники, имеющие доступ к конфиденциальной информации, должны проходить обязательное обучение и инструктаж по вопросам обеспечения секретности. Это включает: знакомство с нормативными документами; обучение правилам работы с секретной информацией; проверку знаний и навыков обращения с конфиденциальными данными. Результаты обучения фиксируются в соответствующих журналах и подтверждаются подписями сотрудников.

Организация должна обеспечить физическую и логическую защиту информации. Это включает: ограничение доступа к помещениям, где хранится секретная информация; использование систем контроля и управления доступом (СКУД); установка видеонаблюдения и охранной сигнализации.

Информационные системы, обрабатывающие конфиденциальные данные, должны быть защищены от несанкционированного доступа. Меры включают: использование антивирусного программного обеспечения; настройку межсетевых экранов и систем обнаружения вторжений; регулярное обновление программного обеспечения и операционных систем.

Передача и хранение секретной информации должны осуществляться с использованием криптографических средств защиты информации, сертифицированных в установленном порядке. Это обеспечивает сохранность данных при их передаче по сетям связи и хранении на носителях информации.

Коммерческие организации, выполняющие государственные заказы, обязаны взаимодействовать с органами государственной власти по вопросам обеспечения секретности. Это включает: получение разрешений и лицензий на работу с государственной тайной; предоставление отчетности о соблюдении режима секретности; участие в проверках и аудитах, проводимых уполномоченными органами.

Нарушение требований по обеспечению секретности может повлечь за собой различные виды ответственности: Дисциплинарная ответственность: применяется к сотрудникам, нарушившим внутренние нормативные документы организации. Административная ответственность: предусмотрена за незаконное разглашение информации, доступ к которой ограничен федеральным законом. Уголовная ответственность: устанавливается за незаконное получение и разглашение сведений, составляющих коммерческую, налоговую или банковскую тайну, если это действие причинило крупный ущерб или совершено из корыстных побуждений.

Список литературы:

1. Федеральный закон от 29 июля 2004 года № 98-ФЗ «О коммерческой тайне».
2. Закон РФ от 21 июля 1993 года № 5485-1 «О государственной тайне».
3. Трудовой кодекс Российской Федерации.
4. Уголовный кодекс Российской Федерации.
5. Кодекс Российской Федерации об административных правонарушениях.
6. Постановление Правительства РФ от 4 сентября 1995 года № 870.
7. Статьи и материалы по вопросам защиты конфиденциальной информации.

