

МУНИЦИПАЛЬНОЕ АВТОНОМНОЕ УЧРЕЖДЕНИЕ  
«ЦЕНТР МОЛОДЕЖНЫХ ИНИЦИАТИВ»  
КОРСАКОВСКОГО ГОРОДСКОГО ОКРУГА САХАЛИНСКОЙ ОБЛАСТИ  
(МАУ «ЦМИ»)

Адрес: 694020, Сахалинская область, г.Корсаков, ул.Восточная, 29/2,  
телефон: 8(42435)4-00-59, e-mail: mbu\_cmi2016@mail.ru



УТВЕРЖДАЮ:  
и.о. директора МАУ «ЦМИ»  
Д.М. Шпачук  
Приказ № 8 от 14.02.2022

ПОРЯДОК ОПРЕДЕЛЕНИЯ УГРОЗ  
И ЗАЩИТЫ ПЕРСОНАЛЬНЫХ ДАННЫХ  
В МУНИЦИПАЛЬНОМ АВТОНОМНОМ УЧРЕЖДЕНИИ  
«ЦЕНТР МОЛОДЕЖНЫХ ИНИЦИАТИВ»  
КОРСАКОВСКОГО ГОРОДСКОГО ОКРУГА САХАЛИНСКОЙ ОБЛАСТИ



## 1. Определение угроз и защита персональных данных

1.1 Под угрозой или опасностью утраты персональных данных работников понимается единичное или комплексное, реальное или потенциальное, активное или пассивное проявление злоумышленных возможностей внешних или внутренних источников угрозы создавать неблагоприятные события, оказывать дестабилизирующее воздействие на защищаемую информацию.

1.2 Риск угрозы любым информационным ресурсам создают стихийные бедствия, экстремальные ситуации, террористические действия, аварии технических средств и линий связи, другие объективные обстоятельства, а также заинтересованные и незаинтересованные в возникновении угрозы лица.

1.3 Защита персональных данных представляет собой жестко регламентированный и динамически технологический процесс, предупреждающий нарушение доступности, целостности, достоверности и конфиденциальности персональных данных и, в конечном счете, обеспечивающий достаточно надежную безопасность информации в процессе управленческой и основной деятельности МАУ «ЦМИ».

1.4 Защита персональных данных работника от неправомерного их использования или утраты должна быть обеспечена директором МАУ «ЦМИ» за счет средств в порядке, установленном федеральным законом.

### 1.5 «Внутренняя защита».

Основным виновником несанкционированного доступа к персональным данным является, как правило, персонал, работающий с документами и базами данных. Регламентация доступа персонала к конфиденциальным сведениям, документам и базам данных входит в число основных направлений организационной защиты информации и предназначена для разграничения полномочий между директором и работниками МАУ «ЦМИ».

Для обеспечения внутренней защиты персональных данных работников необходимо соблюдать ряд мер:

- ограничение и регламентация состава работников, функциональные обязанности которых требуют конфиденциальных знаний;
- строгое избирательное и обоснованное распределение документов и информации между работниками;
- рациональное размещение рабочих мест работников, при котором исключалось бы бесконтрольное использование защищаемой информации;
- знание работником требований нормативно - методических документов по защите информации и сохранении тайны;
- наличие необходимых условий в помещении для работы с конфиденциальными документами и базами данных;
- организация порядка уничтожения информации;
- своевременное выявление нарушения требований разрешительной системы доступа работниками МАУ «ЦМИ»;
- воспитательная и разъяснительная работа с работниками МАУ «ЦМИ» по предупреждению утраты ценных сведений при работе с конфиденциальными документами;
- личные дела могут выдаваться на рабочие места только директору;
- защита персональных данных работника на электронных носителях. Все папки, содержащие персональные данные работника, должны быть защищены паролем.

### 1.6 «Внешняя защита».

Для защиты конфиденциальной информации создаются целенаправленные неблагоприятные условия и труднопреодолимые препятствия для лица, пытающегося совершить несанкционированный доступ и овладение информацией. Целью и результатом



несанкционированного доступа к информационным ресурсам может быть не только овладение ценными сведениями и их использование, но и их видоизменение, уничтожение, внесение вируса, подмена, фальсификация содержания реквизитов документа и др.

Под посторонним лицом понимается любое лицо, не имеющее непосредственного отношения к деятельности МАУ «ЦМИ», посетители, работники других организационных структур. Посторонние лица не должны знать распределение функций, рабочие процессы, технологию составления, оформления, ведения и хранения документов, дел и рабочих материалов в отделе кадров и бухгалтерии.

Для обеспечения внешней защиты персональных данных работников необходимо соблюдать ряд мер:

- порядок приема, учета и контроля деятельности посетителей;
- технические средства охраны, кнопка тревожной сигнализации;
- порядок охраны территории, зданий, помещений;
- требования к защите информации при собеседованиях.

1.7 Все лица, связанные с получением, обработкой и защитой персональных данных, обязаны подписать обязательство о неразглашении персональных данных работников.

1.8 По возможности персональные данные обезличиваются.

1.9 Кроме мер защиты персональных данных, установленных законодательством, работодатели, работники и их представители могут вырабатывать совместные меры защиты персональных данных работников.