**УТВЕРЖДАЮ**
**Руководитель Исполнительного комитета Зеленодольского муниципального района**
**_____Д.В.Грузков**
22.07.2009г.

# ВЫПИСКА из ПОЛОЖЕНИЯ

## об информационной безопасности в Исполнительном комитете Зеленодольского муниципального района.

Положение об информационной безопасности в Исполнительном комитете Зеленодольского муниципального района (далее - Исполком ЗМР) определяет цели и принципы обеспечения информационной безопасности в Исполкоме ЗМР.

Положение об информационной безопасности распространяется на все структурные подразделения Исполкома ЗМР и обязательно для исполнения всеми сотрудниками, работающими в этих подразделениях.

Положение об информационной безопасности в Исполкоме ЗМР предполагает создание совокупности взаимоувязанных нормативных и организационно-распорядительных документов, определяющих порядок обеспечения безопасности информации в информационных системах Исполкома ЗМР, управления и контроля информационной безопасности, а также выдвигающих требования по поддержанию подобного порядка.

Положение об информационной безопасности в Исполкоме ЗМР (далее - Положение) направлено на:

- нормативное регулирование процесса обмена защищаемой информацией в Исполкоме ЗМР с взаимодействующими структурами, юридическими и физическими лицами;
- установление определенного организационно-правового режима использования информационных ресурсов;
- разработку системы нормативных документов, действующих на правах стандартов и определяющих степень конфиденциальности информации, требуемый уровень защищенности объектов информатизации в Исполкоме ЗМР, ответственность должностных лиц и сотрудников за соблюдение этих требований;
- реализацию комплекса организационных, инженерно-технических, технических и аппаратно-программных мероприятий по предупреждению несанкционированных действий с информацией и защиту ее от утечки по техническим каналам;
- предоставление пользователям необходимых сведений для сознательного

поддержания установленного уровня защищенности объектов информатизации;

- организацию постоянного контроля эффективности принятых мер защиты и функционирования системы обеспечения информационной безопасности;
- создание в Исполкоме ЗМР резервов и возможностей по ликвидации последствий нарушения режима защиты информации и восстановления системы обеспечения информационной безопасности.

Настоящий документ разработан в соответствии с требованиями национального стандарта Российской Федерации ГОСТ Р ИСО/МЭК 17799- 2005.

## 1. Цель обеспечения информационной безопасности

Основной целью является обеспечение информационной безопасности в Исполкоме ЗМР, что предполагает эффективное информационное обслуживание и управление всеми средствами комплексной защиты информации, адекватное отражение угроз информационной безопасности, подчиненное единому замыслу.

Главная цель принимаемых мер защиты информации состоит в том, чтобы гарантировать **целостность, достоверность, доступность** и **конфиденциальность** информации во всех ее видах и формах, включая документы и данные, обрабатываемые, хранимые и передаваемые в информационно-вычислительных и телекоммуникационных системах (далее - ИС), независимо от типа носителя этих данных. Организация информационных ресурсов должна обеспечивать их достаточную полноту, точность и актуальность, чтобы удовлетворять потребностям Исполкома ЗМР, не жертвуя при этом основными принципами информационной безопасности, описанными в данном Положении.

Ответственность за организацию и проведение работ по обеспечению информационной безопасности в Исполкоме ЗМР несет Руководитель Исполнительного комитета Зеленодольского муниципального района. Разработку проектов объектов информатизации в защищенном исполнении и их эксплуатацию с учетом требований по защите информации, методическое руководство и контроль за эффективностью предусмотренных мер защиты осуществляет специалист, на которого возложено исполнение обязанностей по информационной безопасности.

## 2. Объекты информационной безопасности

Объектом защиты в контексте данного Положения являются информационные ресурсы Исполкома ЗМР, обрабатываемые в информационных системах и ее функциональных подсистемах, содержащие сведения доступ к которым ограничен, и используемые в процессах сбора, обработки, накопления, хранения и распространения в границах информационных систем Исполкома ЗМР.

Основными объектами защиты являются:

информационные ресурсы Исполкома ЗМР, содержащие сведения, отнесенные к государственной тайне;

информационные ресурсы Исполкома ЗМР, ограниченного распространения, в том числе, содержащие конфиденциальные сведения;

информационные ресурсы Исполкома ЗМР, представляющие коммерческую ценность;

программные информационные ресурсы Исполкома ЗМР, а именно: прикладное программное обеспечение, системное программное обеспечение, инструментальные средства и утилиты;

физические информационные ресурсы Исполкома ЗМР: компьютерное аппаратное обеспечение всех видов; носители информации всех видов (электронные, бумажные и проч.);

все расходные материалы и аксессуары, которые прямо или косвенно взаимодействуют с компьютерным аппаратным и программным обеспечением;

технические сервисы Исполкома ЗМР (отопление, освещение, энергоснабжение, кондиционирование воздуха и т.п.).

Следует также отметить, что указанные выше основные объекты защиты являются наиболее ценными ресурсами, и, следовательно, по отношению к ним должны применяться самые эффективные правила и методы защиты. Их доступность, целостность и конфиденциальность могут иметь особое значение для обеспечения имиджа Исполкома ЗМР, эффективности его функционирования и т.д. Доступность, целостность и конфиденциальность в обязательном порядке должны учитываться при разработке организационно-распорядительной документации по обеспечению информационной безопасности для системы в целом и для каждого ее ресурса в отдельности.

## 3. Задачи обеспечения информационной безопасности

Основными задачами обеспечения информационной безопасности Исполкома ЗМР являются:

инвентаризация и систематизация всех информационных ресурсов Исполкома ЗМР;

обеспечение безопасности информационных ресурсов Исполкома ЗМР, уменьшение риска их случайной или намеренной порчи, уничтожения или хищения;

сведение к минимуму финансовых, временных и прочих потерь, связанных с нарушением информационной безопасности и физическими неисправностями аппаратного и программного обеспечения, а также осуществление мониторинга и реагирование по случаям инцидентов;

обеспечение безопасной, четкой и эффективной работы сотрудников Исполкома ЗМР с его информационными ресурсами;

сведение к разумному минимуму финансовых затрат на поддержание функционирования аппаратного и программного обеспечения и автоматизированной системы в целом на должном уровне (сюда относятся крупные и мелкие обновления программного и аппаратного обеспечения, бесперебойное обеспечение системы расходными материалами и проч.);

сведение пользования информационными ресурсами к единой системе организационно-распорядительной документации.