ТАТАРСТАН РЕСПУБЛИКАСЫ

ЧИРМЕШЭН МУНИЦИПАЛЬ
РАЙОНЫ
БАШЛЫГЫ

РЕСПУБЛИКА ТАТАРСТАН

ГЛАВА
ЧЕРЕМШАНСКОГО
МУНИЦИПАЛЬНОГО РАЙОНА

423100, ЧИРМЕШЭН АВЫЛЫ, СОВЕТ УРАМЫ,32

тел.+7(84316) 2-51-00
тел./факс +7(84316) 2-59-
email:cheremshan@kremlin.tatarstan.ru

423100, село ЧЕРЕМШАН,УЛ.СОВЕТСКАЯ, 32

№ 47 «22» июля 2009 г.

КАРАР
ПОСТАНОВЛЕНИЕ

Об образовании рабочей группы по обеспечению безопасности персональных данных

В соответствии с Федеральным законом от 27 июля 2006 года № 152-ФЗ «О персональных данных», постановлением Правительства Российской Федерации от 17 ноября 2007 года № 781 «Об утверждении Положения об обеспечении безопасности персональных данных при их обработке в информационных системах персональных данных», распоряжения Кабинета Министров Республики Татарстан от 17 января 2008 года № 19-р **ПОСТАНОВЛЯЮ**:

1. Образовать рабочую группу по защите персональных данных при их обработке в информационных системах в органах местного самоуправления и подведомственных им учреждениях в следующем составе:

Ахмадуллин Р.И. — заместитель руководителя Исполнительного комитета Черемшанского муниципального района по экономическим вопросам, председатель рабочей группы

Члены комиссии:

Аглиуллин М.Х. — начальник отдела территориального развития Исполнительного комитета Черемшанского муниципального района

Галимов И.Б. — начальник отдела культуры Исполнительного комитета Черемшанского муниципального района

Маслахутдинов И.С. — специалист 1 разряда Управления по информационному обеспечению системы ГАС «выборы» (по согласованию)

Митрюхин В.В. — начальник организационного отдела Совета Черемшанского муниципального района

Никонова Н.Д. — начальник отдела ЗАГС Исполнительного комитета Черемшанского муниципального района

Хакимов Х. Ш. — начальник отдела образования Исполнительного комитета Черемшанского муниципального района.

2. Утвердить прилагаемые:

- Политику информационной безопасности персональных данных в органах местного самоуправления Черемшанского муниципального района Республики Татарстан (приложение № 1);

- Положение о защите персональных данных в органах местного самоуправления Черемшанского муниципального района Республики Татарстан (приложение № 2).

3. Назначить ответственным лицом за информационную безопасность персональных данных в органах местного самоуправления Черемшанского муниципального района Республики Татарстан председателя рабочей группы, заместителя руководителя Исполнительного комитета Ахмадуллина Р.И.

Глава муниципального района **М.З. ШАКИРОВ**

Подготовил:
Начальник организационного
отдела Совета района В.В. Митрюхин

Проверил:
Начальник юридического отдела Н.К. Исламов

Приложение №1 к постановлению
Главы Черемшанского муниципального
района Республики Татарстан
№ 47 от «22» июля 2009 года

Политика информационной безопасности персональных данных в органах местного самоуправления Черемшанского муниципального района.

1. Общие положения.

Политика информационной безопасности персональных данных в органах местного самоуправления Черемшанского муниципального района Республики Татарстан (далее – Политика ИБ) предполагает создание совокупности взаимоувязанных нормативных и организационно-распорядительных документов, определяющих порядок обеспечения безопасности информации в информационных системах в органах местного самоуправления и подведомственных организациях органов местного самоуправления Черемшанского муниципального района, управление и контроль информационной безопасности, а также выдвигающих требования по поддержанию подобного порядка.

Политика ИБ отражает позицию руководства органов местного самоуправления Черемшанского муниципального района по вопросу обеспечения информационной безопасности.

Политика ИБ направлена на:

- нормативное регулирование процесса обмена защищаемой информацией 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, 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 резервов и возможностей по ликвидации последствий

нарушения режима защиты информации и восстановления системы обеспечения информационной безопасности.

2. Цель обеспечения информационной безопасности.

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 -информационные системы), независимо от типа носителя этих данных. Организация информационных ресурсов должна обеспечивать их достаточную полноту, точность и актуальность, чтобы удовлетворять потребности, не жертвуя при этом основными принципами информационной безопасности, описанными в данной Политике.

Обеспечение информационной безопасности предполагает эффективное информационное обслуживание и управление всеми средствами комплексной защиты информации, адекватное отражение угроз информационной безопасности, подчиненное единому замыслу.

Ответственность за организацию и проведение работ по обеспечению информационной безопасности несет **Председатель рабочей группы по обеспечению безопасности персональных данных при их обработке в информационных системах**. В органах местного самоуправления осуществляется разработка проектов объектов информатизации в защищенном исполнении и их эксплуатация с учетом требований по защите информации. Методическое руководство и контроль за эффективностью предусмотренных мер защиты осуществляет соответствующий специалист по информационной безопасности.

3. Объекты информационной безопасности.

Объектом защиты в контексте данной Политики являются информационные ресурсы органов местного самоуправления и подведомственных им структур, 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. Основными объектами защиты являются:

-информационные ресурсы, содержащие сведения, отнесенные к государственной тайне;

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

- информационные ресурсы, представляющие коммерческую ценность;

- программные информационные ресурсы, именно: прикладное программное обеспечение, системное программно обеспечение, инструментальные средства и утилиты;
- физические информационные ресурсы - компьютерное аппаратное обеспечение всех видов;
- носители информации все видов (электронные, бумажные и проч.);
- все расходные материалы и аксессуары, которые прямо или косвенно взаимодействуют с компьютерным аппаратным и программным обеспечением;
- технические сервисы (отопление, освещение, энергоснабжение, кондиционирование воздуха и т.п.).

Указанные выше основные объекты защиты являются наиболее ценными ресурсами и следовательно, по отношению к ним должны применяться самые эффективные правила и методы защиты. И доступность, целостность и конфиденциальность могут иметь особое значение для обеспечения имиджа, 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.

4. Задачи обеспечения информационной безопасности.

Основными задачами обеспечения информационной безопасности являются:

- инвентаризация и систематизация всех информационных ресурсов ;
- обеспечение безопасности информационных ресурсов;
- 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 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.

5. Принципы обеспечения информационной безопасности