ГЛАВА САРМАНОВСКОГО
МУНИЦИПАЛЬНОГО РАЙОНА
РЕСПУБЛИКИ ТАТАРСТАН

ТАТАРСТАН РЕСПУБЛИКАСЫ
САРМАН МУНИЦИПАЛЬ
РАЙОНЫ БАШЛЫГЫ

ПОСТАНОВЛЕНИЕ **КАРАР**

09.03.2016г. с. Сарманово № 66

Об информационной безопасности в
Совете и Исполнительном комитете
Сармановского муниципального района

В соответствии с Федеральным законом от 27 июля 2006 года № 149-ФЗ «Об информации, информационных технологиях и о защите информации», Федеральным законом Российской Федерации от 27 июля 2006 г. N 152-ФЗ «О персональных данных», и в целях осуществления постоянного контроля соблюдения требований по защите информации

ПОСТАНОВЛЯЮ:

1.Утвердить:

- политику информационной безопасности Совета и Исполнительного комитета Сармановского муниципального района (Приложение 1);
- положение о специалисте по информационной безопасности (Приложение 2);
- регламент доступа в помещения с серверным и телекоммуникационным оборудованием (Приложение 3);
- инструкцию по обеспечению безопасности информации пользователя ИТ-инфраструктуры (Приложение 4);
- положение о категорировании информационных ресурсов (Приложение 5);
- согласие работника на обработку персональных данных (Приложение 6).

2. Назначить ответственными:

- Руководителя аппарата Совета за организацию и контроль работ по обеспечению безопасности персональных данных;
- Управляющего делами Исполнительного комитета за организацию и контроль работ по обеспечению безопасности информации;
- Главного специалиста Исполнительного комитета специалистом по информационной безопасности.

4. Контроль за исполнением настоящего постановления оставляю за собой.

Глава
муниципального района Ф.М.Хуснуллин

Приложение 1
Для служебного пользования
Экз. № ___

УТВЕРЖДЕНА
Постановлением Главы
Сармановского
муниципального района
от «09» марта 2016 г. № 66

Политика информационной безопасности

1. Общие положения

Политика информационной безопасности Совета и Исполнительного комитета Сармановского муниципального района предполагает создание совокупности взаимоувязанных нормативных и организационно-распорядительных документов, определяющих порядок обеспечения безопасности информации в информационных системах Совета и Исполнительного комитета Сармановского муниципального района, управления и контроля информационной безопасности, а также выдвигающих требования по поддержанию подобного порядка.

Политика информационной безопасности отражает позицию руководства Совета и Исполнительного комитета Сармановского муниципального района по вопросу обеспечения информационной безопасности министерства.

Политика информационной безопасности Совета и Исполнительного комитета Сармановского муниципального района направлена на:

нормативное регулирование процесса обмена защищаемой информацией Совета и Исполнительного комитета Сармановского муниципального района с взаимодействующими структурами, юридическими и физическими лицами;

установление определенного организационно-правового режима использования информационных ресурсов Совета и Исполнительного комитета Сармановского муниципального района;

разработку системы нормативных документов Совета и Исполнительного комитета Сармановского муниципального района, действующих на правах стандартов и определяющих степень конфиденциальности информации, требуемый уровень защищенности объектов информатизации Совета и Исполнительного комитета Сармановского муниципального района, 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 Совета и Исполнительного комитета Сармановского муниципального района;

организацию постоянного контроля эффективности принятых мер защиты и функционирования системы обеспечения информационной безопасности Совета и Исполнительного комитета Сармановского муниципального района;

создание в Совете и Исполнительном комитете Сармановского муниципального района 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.

2. Цель обеспечения информационной безопасности

Основной целью является обеспечение информационной безопасности Совета и Исполнительного комитета Сармановского муниципального района, 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 Совета и Исполнительного комитета Сармановского муниципального района 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) Совета и Исполнительного комитета Сармановского муниципального района, независимо от типа носителя этих данных. Организация информационных ресурсов должна обеспечивать их достаточную полноту, точность и актуальность, чтобы удовлетворять потребности Совета и Исполнительного комитета Сармановского муниципального района, не жертвуя при этом основными принципами информационной безопасности, описанными в данной Политике.

Ответственность за организацию и проведение работ по обеспечению информационной безопасности Совета и Исполнительного комитета Сармановского муниципального района несет Глава муниципального района. Главный специалист Исполнительного комитета осуществляет 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 по информационной безопасности Исполнительного комитета Сармановского муниципального района.

3. Объекты информационной безопасности соответствующего Министерства

Объектом защиты в контексте данной Политики являются информационные ресурсы Совета и Исполнительного комитета Сармановского муниципального района, 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 Совета и Исполнительного комитета Сармановского муниципального района.

Основными объектами защиты Совета и Исполнительного комитета Сармановского муниципального района являются:

информационные ресурсы Совета и Исполнительного комитета Сармановского муниципального района, содержащие сведения, отнесенные к государственной тайне;

информационные ресурсы Совета и Исполнительного комитета Сармановского муниципального района, ограниченного распространения, в том числе, содержащие конфиденциальные сведения;

информационные ресурсы Совета и Исполнительного комитета Сармановского муниципального района, представляющие коммерческую ценность;

программные информационные ресурсы Совета и Исполнительного комитета Сармановского муниципального района, а именно: прикладное программное обеспечение, системное программное обеспечение, инструментальные средства и утилиты;

физические информационные ресурсы Совета и Исполнительного комитета Сармановского муниципального района: 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 Совета и Исполнительного комитета Сармановского муниципального района (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 Совета и Исполнительного комитета Сармановского муниципального района, 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 Совета и Исполнительного комитета Сармановского муниципального района являются:

инвентаризация и систематизация всех информационных ресурсов Совета и Исполнительного комитета Сармановского муниципального района;

обеспечение безопасности информационных ресурсов Совета и Исполнительного комитета Сармановского муниципального района: 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 Совета и Исполнительного комитета Сармановского муниципального района 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 Совета и Исполнительного комитета Сармановского муниципального района

При построении системы защиты необходимо придерживаться следующих принципов:

применение разнородных систем обеспечения информационной безопасности;

достоинства одних частей системы обеспечения информационной безопасности должны перекрывать недостатки других;

система обеспечения информационной безопасности должна строиться многоуровневой;

в зоне максимальной безопасности должны располагаться особо важные информационные ресурсы;

непрерывность и целенаправленность процесса обеспечения информационной безопасности;

усиление защиты информации во время нештатных ситуаций;

обеспечение возможности регулирования уровня информационной безопасности без изменения функциональной базы системы информационной безопасности;

обеспечение простоты в применении механизмов защиты для рядовых сотрудников Совета и Исполнительного комитета Сармановского муниципального района.

6. Оценка рисков

Для оценки рисков при составлении и последующем пересмотре организационно-распорядительных документов необходимо систематически рассматривать следующие аспекты:

ущерб, который может нанести деятельности Совета и Исполнительного комитета Сармановского муниципального района серьезное нарушение информационной безопасности, с учетом возможных последствий нарушения конфиденциальности, целостности и доступности информации;

реальную вероятность такого нарушения защиты в свете превалирующих угроз и средств контроля.

7. Требования в отношении обучения вопросам информационной безопасности

Основной целью обучения является:

обеспечение уверенности в осведомленности сотрудников Совета и Исполнительного комитета Сармановского муниципального района об угрозах и проблемах, связанных с информационной безопасностью, об ответственности в соответствии с законодательством;

знание сотрудниками правильного использования средств обработки информации прежде чем им будет предоставлен доступ к информации или услугам;

оснащение сотрудников Совета и Исполнительного комитета Сармановского муниципального района всем необходимым для соблюдения требований политики безопасности Совета и Исполнительного комитета Сармановского муниципального района при выполнении служебных обязанностей.

Сотрудники Совета и Исполнительного комитета Сармановского муниципального района должны знать и выполнять требования организационно-распорядительных документов (в части касающейся) Совета и Исполнительного комитета Сармановского муниципального района в области информационной безопасности, требования обеспечения безопасности обработки информации на средствах вычислительной техники, правила работы в сети Интернет.

Сотрудники Совета и Исполнительного комитета Сармановского муниципального района должны уметь работать с системой электронного документооборота; операционными системами MS Wndows на уровне пользователя, антивирусным программным обеспечением, офисным программным обеспечением (MS Word, MS Excel, MS Power Point), должны уметь пользоваться встроенной справкой.

Системный администратор вместе с специалистом по информационной безопасности должны обучать сотрудников Совета и Исполнительного комитета Сармановского муниципального района правильному использованию средств обработки защиты информации, чтобы свести к минимуму возможные риски безопасности.

Все сотрудники Совета и Исполнительного комитета Сармановского муниципального района и, при необходимости, пользователи третьей стороны, должны пройти соответствующее обучение и получать на регулярной основе обновленные варианты политик информационной безопасности, принятых в Совете и Исполнительного комитета Сармановского муниципального района.

8. Правила физической защиты

Перед внедрением и использованием нового аппаратного, программного обеспечения или иного ранее не использовавшегося информационного ресурса необходимо разработать для него правила обеспечения безопасности и использовать их наряду с правилами, изложенными в данном разделе.

Перед установкой и использованием какого-либо компьютерного аппаратного обеспечения в обязательном порядке следует ознакомиться с информацией, предоставленной разработчиком (продавцом), и строго ей следовать.

Перед проведением крупной модернизации или ремонта, перед выполнением манипуляций непосредственно с носителями информации необходимо выполнить резервное копирование данных.

После выполнения процесса модернизации аппаратного и/или программного обеспечения необходимо обязательно провести внеплановое техническое обслуживание всей системы.

При размещении компьютерного оборудования в помещении, а также в процессе его эксплуатации приоритетным является обеспечение для него безопасного функционирования, соответствующего положениям, изложенным в прилагаемой к нему документации. В период простоя устройства необходимо обеспечить сохранность его работоспособности и внешнего вида.

Все приобретенное компьютерное аппаратное и программное обеспечение должно регистрироваться в специальном журнале с указанием подробной информации о его покупке. Также следует тщательно регистрировать все действия по модернизации компьютерного аппаратного и программного обеспечения.

Всю документацию на компьютерное оборудование и программное обеспечение (гарантийные обязательства производителей/продавцов, руководства пользователей (User's Manual), регистрационные карточки, кассовые и товарные чеки и проч.) должны обязательно сохраняться после покупки и храниться в надежном, защищенном от света и других вредоносных воздействий месте в упаковке.

Следует в полном объеме и неукоснительно соблюдать правила эксплуатации тех или иных аппаратных компьютерных компонентов.

Техническое обслуживание компьютерного оборудования и программного обеспечения (физическая чистка оборудования, поддержание программного обеспечения в работоспособном состоянии и т.д.) следует производить регулярно, желательно в соответствии с заранее составленным расписанием и с учетом рекомендаций разработчиков данного оборудования и программ (с данными рекомендациями следует внимательно ознакомиться до выполнения каких-либо действий по обслуживанию).

Техническим обслуживанием считаются также и мероприятия по резервному копированию данных, которые должны неукоснительно исполняться. Они должны выполняться строго регулярно и не реже, чем раз в неделю. Если это возможно, стоит сделать повторную копию данных и разместить ее на хранение отдельно от первой. Сразу же после проведения резервного копирования данных необходимо

каким-либо способом убедиться в работоспособности и корректности полученной копии.

Резервному копированию в обязательном порядке подлежат:

все конфиденциальные данные сотрудников в автоматизированной системе;

все исходные материалы для разработки собственного программного обеспечения и прочих проектов;

такие данные системы, без которых невозможна ее нормальная работа;

все прочие важные данные, которые записаны на физически ненадежных носителях информации и носителях, поддерживающих операции перезаписи;

любые другие данные согласно решению уполномоченных сотрудников Совета и Исполнительного комитета Сармановского муниципального района.

Во время резервного копирования данных, а также во время записи любой информации на носители информации однократной записи, нельзя производить другие виды работ на той компьютерной системе, при помощи которой осуществляется эта запись.

Все носители (электронные, бумажные и все другие) с конфиденциальной информацией и резервными копиями этой и другой информации сотрудника Совета и Исполнительного комитета Сармановского муниципального района должны храниться в недоступном для посторонних, защищенном от света и других вредоносных воздействий месте с соблюдением правил безопасного хранения для данного вида носителя информации. Носителям с особо ценной информацией следует уделять повышенное внимание.

Все расходные материалы следует использовать максимально эффективно, не допуская нерационального их использования. Все расходные материалы (используемые в данный момент и неиспользуемые) необходимо хранить в строгом соответствии с правилами их хранения.

Желательно предпринять ряд мер по энергосбережению для тех устройств, которые временно не используются или находятся в состоянии ожидания.

Запрещается курить, употреблять пищу и напитки непосредственно вблизи компьютера. Необходимо предпринять меры, чтобы обезопасить компьютерное оборудование от повреждения в данном случае.

В течение внедрения и использования нового аппаратного, программного обеспечения или иного ранее не использовавшегося информационного ресурса необходимо приложить все усилия к тому, чтобы научиться эффективно его применять.

Необходимо в обязательном порядке записать все наиболее важные установки и настройки системы в состоянии ее нормального (штатного) функционирования. Подобные записи приравниваются к аппаратно/программной документации, и должны соответствующим образом обслуживаться.

Необходимо размещать системы вывода информации (мониторы, дисплеи и т.д.) компьютеров так, чтобы они не были видны со стороны двери, окон и тех мест в помещениях, которые не контролируются.

Необходимо предпринять ряд мер, благодаря которым компьютерные системы пользователя будут обеспечены стабильным электропитанием. Обязательным

является использование хотя бы самых простых средств по обеспечению надежности электропитания системы (сетевые фильтры, заземление и т.д.).

При возникновении какой-либо аварийной ситуации необходимо немедленно прекратить эксплуатацию аварийного устройства. Немедленно поставить в известность системного администратора. Системному администратору в кратчайшие сроки организовать мероприятия по его ремонту или замене.

Следует составить подробные технологические схемы для проведения различного рода мероприятий, связанных с аппаратным и программным обеспечением (техническое обслуживание, правила техники безопасности, резервное копирование данных и т.п.).

Необходимо рассмотреть возможность применения различных систем автоматизированного мониторинга текущего состояния аппаратных информационных ресурсов, и при первой же возможности внедрить их, по крайней мере, на наиболее важных и ответственных участках.

В течение процесса списания компьютерной техники, носителей информации и др. необходимо позаботиться о том, чтобы после выполнения процедуры переноса основных информационных ресурсов со списываемой техники, было произведено полное и безвозвратное уничтожение содержащейся на ней конфиденциальной и любой другой информации.

Необходимо обязательно разработать план действий по продолжению работы и обеспечению безопасности данных на случай, если выйдут из строя какие-либо аппаратные и/или программные части компьютерной системы. Данный план должен систематически проверяться на актуальность и при необходимости пересматриваться.

9. Правила внешнего доступа

После установки системы и перед первым выходом в сеть необходимо в обязательном порядке принять комплекс мер по установлению защиты от вредоносного воздействия сети.

В системе должны быть предприняты все возможные меры для предотвращения распространения в ней компьютерных вирусов, «червей» и прочей потенциально опасной для ее безопасности информации. Все сотрудники Совета и Исполнительного комитета Сармановского муниципального района обязаны принимать участие в реализации этих мер и никакими своими действиями не должны препятствовать их проведению.

Необходимо строго контролировать с помощью соответствующего программного обеспечения (антивирус, брандмауэр и проч.) всю входящую и исходящую информацию на наличие вирусов и прочей потенциально опасной информации. Необходимо также тщательно настроить параметры безопасности того программного и аппаратного обеспечения, которое непосредственно будет иметь доступ в сеть.

Система должна подвергаться периодической проверке антивирусными средствами (не реже чем раз в месяц) и другими средствами, обеспечивающими безопасность в системе (если таковые имеются). В случае обнаружения при

проведении антивирусной проверки зараженных компьютерными вирусами файлов сотрудники Совета и Исполнительного комитета Сармановского муниципального района обязаны: приостановить работу на компьютере, немедленно поставить в известность о факте обнаружения зараженных вирусом файлов руководителя отдела, владельца зараженных файлов, смежные отделы, использующие эти файлы в работе, а также системного администратора, специалиста по информационной безопасности.

Все внешние носители информации, полученные из сомнительных или неизвестных источников должны подвергаться полному антивирусному сканированию перед использованием.

Необходимо регулярно обновлять версии программного обеспечения, связанного с обеспечением безопасности системы; устанавливать официальные обновления программ, которые имеют прямое или косвенное отношение к работе с сетью. Сюда же относятся и обновления, связанные с управлением аппаратным обеспечением системы (драйверы устройств и т.п.).

При обнаружении зараженных вирусами данных, эти данные должны немедленно и безвозвратно удаляться. Исключение составляют лишь важные данные, для которых имеет смысл попробовать применить процедуры восстановления.

Следует с большой осторожностью относится к программам, в которых присутствуют определенного рода уязвимости для несанкционированного проникновения, или же в которых включены особые привилегии для их разработчиков.

Необходимо внимательно проанализировать систему данных сотрудника и обеспечить ее структурированное хранение на носителях информации. Все данные должны классифицироваться согласно их применению или же по другому, четко установленному сотрудником критерию (например, критериями могут служить соображения конфиденциальности данных, место из размещения и способ пересылки).

10. Правила доступа в Интернет

Программное обеспечение, обеспечивающее защиту системы от проникновения, должно быть задействовано в полном объеме на протяжении всего сеанса связи с Интернетом.

Допускается временное отключение части программного обеспечения, обеспечивающего защиту системы, в тех случаях, когда без этого невозможно выполнить какой-либо вид работы. После выполнения данного вида работ отключенные части системы защиты должны быть вновь задействованы.

Сотрудники Совета и Исполнительного комитета Сармановского муниципального района допускаются к использованию Интернета только после прохождения инструктажа, в котором разъяснялась бы Политика безопасности данной системы в отношении глобальной сети.

Сотрудники Совета и Исполнительного комитета Сармановского муниципального района должны стараться предоставлять о себе как можно меньше

информации в сеть, а тем более не должны разглашать любую конфиденциальную информацию.

Все файлы, полученные из Интернета, перед их использованием должны пройти дополнительную антивирусную проверку.

После каждого сеанса связи с Интернетом необходимо проводить очистку системы от ненужных служебных данных, которые появились в результате соединения с сетью.

Все данные, полученные из Интернета должны систематизироваться и сохраняться.

11. Правила безопасности электронной почты

Все наиболее важные сообщения электронной почты должны архивироваться, особенно те сообщения, которые присланы официальными группами технической поддержки каких-либо информационных ресурсов. Также регулярной архивации должна подвергаться информация, касающаяся данных о тех сотрудниках, с которыми осуществляется связь средствами электронной почты (адресные книги и т.д.).

Все ранее сохраненные почтовые сообщения, потерявшие свою актуальность, должны быть тщательным образом безвозвратно уничтожены со всех носителей информации.

Необходимо в обязательном порядке сканировать каждое исходящее и получаемое сообщение электронной почты на наличие потенциально опасного содержимого (вирусы, «черви» и т.д.). Почтовые сообщения, не удовлетворяющие установленным требованиям, должны немедленно и безвозвратно удаляться.

Необходимо на всех используемых почтовых ящиках установить, при необходимости, ограничения на содержимое и размер принимаемых сообщений и отсеивать те сообщения, которые не удовлетворяют установленным критериям.

После отправки письма по электронной почте необходимо хранить его до тех пор, пока не будет уверенности (подтверждения) в том, что оно достигло получателя. Это же касается и любых других способов передачи информации. Все файлы (особенно исполнимые и файлы больших размеров), полученные вместе с сообщением электронной почты без какого-либо запроса со стороны сотрудника Совета и Исполнительного комитета Сармановского муниципального района (особенно от неизвестного адресата) должны немедленно и безвозвратно удаляться без оценки их полезности. При этом каждый подобный факт должен быть зарегистрирован. Если нет полной уверенности в необходимости удаления данного сообщения, необходимо, в случае если адресат известен и только в этом случае, дополнительно связаться с ним (не по электронной почте) и попросить у него подтверждения в посылке сообщения.

Сотрудники Совета и Исполнительного комитета Сармановского муниципального района не должны участвовать в рассылке посланий, передаваемых по цепочке, не должны отвечать на оскорбительные и провокационные сообщения. Такие послания должны быть сначала переданы службам технической поддержки используемых почтовых сервисов для анализа, а после этого – безвозвратно удалены

из системы. Также необходимо принять все возможные меры по обеспечению прекращения получения из данного источника подобной информации в будущем.

12. Правила управления доступом

В отношении всех основных и не основных (гости и проч.) сотрудников Совета и Исполнительного комитета Сармановского муниципального района необходимо осуществлять комплекс мер по обеспечению их работы в автоматизированной системе Совета и Исполнительного комитета Сармановского муниципального района, в частности регистрацию, выделение определенных информационных ресурсов и установление четких не избыточных, а только необходимых, прав доступа к ним.

Служба регистрации должна обеспечить положительную аутентификацию. Это даст гарантию того, что законный пользователь получит доступ к системе.

Необходимо в обязательном порядке регистрировать все удачные и неудачные попытки входа в систему, а также вести аудит доступа сотрудников Совета и Исполнительного комитета Сармановского муниципального района к ее объектам и периодически просматривать результаты его работы.

При первой же необходимости работы с системой при помощи удаленного доступа или же с локальной сетью необходимо разработать правила безопасности, регламентирующие данные виды работ.

Использование имен и паролей для доступа к информационным ресурсам:

необходимо использовать пароли везде, где это целесообразно;

следует придерживаться следующих правил составления и использования паролей - пароль должен состоять не менее чем из шести символов, состоять из произвольных комбинаций букв, цифр и других символов или же представлять собой бессмысленную комбинацию слов, включающую буквы верхнего регистра;

необходимо менять все пароли не реже, чем раз в два месяца (желательно делать это не по графику), при этом использовать пароли повторно не разрешается;

запрещено использовать одинаковые пароли для доступа к разным информационным ресурсам;

пароли необходимо хранить в надежном, недоступном для посторонних месте или же использовать специальные аппаратные средства для их хранения;

хранение паролей осуществляется операционной системой, и установленный ею уровень защиты не может быть ослаблен;

запрещено сообщать свои пароли третьим лицам в какой бы то ни было форме;

пароли запрещается писать на компьютерных терминалах, помещать в общедоступные места;

необходимо заменить все пароли, назначенные системой по умолчанию, на собственные, а потом, если это возможно, отключить возможность доступа к данному ресурсу по стандартному паролю;

все имена и пароли для доступа к каким-либо информационным ресурсам, которые не используются, подлежат надежной блокировке;

система должна предотвращать попытки регистрации и перерегистрации тех сотрудников, чьи имена и пароли для входа в систему не соответствуют установленным правилам;

при получении доступа к какому-либо информационному ресурсу при помощи процесса авторизации по имени и паролю сотрудник не должен произносить эти данные вслух при вводе их в систему;

изменять пароли необходимо всякий раз, когда есть указания на возможную компрометацию систем или паролей.

13. Управление непрерывностью работы Совета и Исполнительного комитета Сармановского муниципального района

Основной целью управления непрерывностью работы Совета и Исполнительного комитета Сармановского муниципального района является противодействие прерывания работы и защита рабочих процессов от последствий при значительных сбоях или бедствиях.

Необходимо обеспечивать управление непрерывностью работы с целью минимизации отрицательных последствий, вызванных нарушениями безопасности. Последствия от нарушений безопасности и отказов в обслуживании необходимо анализировать, по результатам анализа разрабатывать и внедрять планы обеспечения непрерывности работы с целью восстановления рабочих процессов в течение требуемого времени при их нарушении. Такие планы следует поддерживать и применять на практике. Должна быть выработана стратегия непрерывности рабочего процесса в соответствии с согласованными целями и приоритетами. Необходимо чтобы планирование непрерывности работы начиналось с идентификации событий, которые могут быть причиной прерывания работы, например отказ оборудования, наводнение или пожар. Планирование должно сопровождаться оценкой рисков с целью определения последствий этих прерываний (как с точки зрения масштаба повреждения, так и периода восстановления). Оценка риска должна распространяться на все рабочие процессы и не ограничиваться только средствами обработки информации. В зависимости от результатов оценки рисков необходимо разработать стратегию для определения общего подхода к обеспечению непрерывности работы. Разработанный план должен быть утвержден руководством Совета и Исполнительного комитета Сармановского муниципального района. Необходимо, чтобы план обеспечения непрерывности работы предусматривал следующие мероприятия по обеспечению информационной безопасности:

определение и согласование всех обязанностей должностных лиц и процедур на случай чрезвычайных ситуаций;

внедрение в случае чрезвычайных ситуаций процедур, обеспечивающих возможность восстановления рабочего процесса в течение требуемого времени;

особое влияние следует уделять оценке зависимости работы от внешних факторов и существующих контрактов;

документирование согласованных процедур и процессов;

соответствующее обучение сотрудников действиям при возникновении чрезвычайных ситуаций, включая кризисное управление.

Необходимо, чтобы план обеспечения непрерывности работы соответствовал требуемым целям работы.

14. Ответственность за нарушение политики безопасности

Все сотрудники Совета и Исполнительного комитета Сармановского муниципального района несут ответственность за нарушение требований настоящей Политики информационной безопасности согласно действующему законодательству в области защиты информации.

15. Сопровождение правил

Все без исключения положения данного документа имеют одинаково равную силу и должны неукоснительно соблюдаться.

Политика информационной безопасности должна в обязательном порядке периодически перечитываться и пересматриваться (не реже чем один раз в год).

Ежемесячно должна проводиться оценка текущего состояния имеющихся у сотрудников информационных ресурсов. В результате этой оценки в соответствующие документы по безопасности должны вноситься необходимые изменения (если они есть).

При проведении каких-либо изменений в данных правилах, соответствующие изменения, при необходимости, должны производиться и в других документах, касающихся обеспечения безопасности.

Если возникли непредвиденные обстоятельства, требующие срочного пересмотра Политики информационной безопасности, то такой пересмотр может быть осуществлен до планового пересмотра.

При возникновении серьезных проблем с безопасностью системы (например, при успешном взломе системы безопасности) возникшая проблема должна быть немедленно проанализирована, а организационно-распорядительные документы по информационной безопасности – пересмотрены в соответствии с проведенным анализом. При этом нужно рассматривать проблему в целом и излишне не фокусировать внимание на отдельных деталях.

Копия настоящей Политики должна находиться в доступном для сотрудников Совета и Исполнительного комитета Сармановского муниципального района месте.

Приложение 2
Для служебного пользования
Экз. № ___

УТВЕРЖДЕН
Постановлением Главы
Сармановского
муниципального района
от «09» марта 2016 г.
№ 66

Положение о специалисте по информационной безопасности

I. Общие положения

1.1. Настоящее Положение о специалисте по информационной безопасности (далее - Положение) определяет основные цели, функции и права специалиста по информационной безопасности в Совете и Исполнительном комитете Сармановского муниципального района

1.2. Специалист по информационной безопасности назначается постановлением Главы Сармановского муниципального района на основании Положения о государственной системе защиты информации в Российской Федерации от иностранных технических разведок и от ее утечки по техническим каналам, утвержденного постановлением Совета Министров - Правительства Российской Федерации от 15 сентября 1993 г. № 912-51.

1.3. Специалист по информационной безопасности проводит свою работу согласно нормативно- методическим документам Федеральной службы по техническому и экспортному контролю (Гостехкомиссии) России.

Непосредственное руководство работой специалиста по информационной безопасности осуществляет руководитель аппарата Совета Сармановского муниципального района, курирующий вопросы защиты информации

Назначение и освобождение от должности специалиста по информационной безопасности производится Главой муниципального района.

Примечание:

специалист по защите информации может быть назначен, по усмотрению Главы муниципального района, из числа сотрудников одного из подразделений Совета и Исполнительного комитета Сармановского муниципального района.

1.5. Специалист по информационной безопасности назначается из числа сотрудников Совета и Исполнительного комитета Сармановского муниципального района, имеющих опыт работы по основной деятельности Совета и Исполнительного комитета Сармановского муниципального района или в области защиты информации и отвечающих требованиям квалификационных характеристик на специалистов по комплексной защите информации.

1.6. Специалист по информационной безопасности приравнивается по оплате труда, льготам и премированию к соответствующим категориям

1.7. Специалист по информационной безопасности проводит свою работу во взаимодействии с соответствующими режимно-секретными подразделениями Совета и Исполнительного комитета Сармановского муниципального района, отделом информационной безопасности Министерства информатизации и связи Республики Татарстан, Федеральной службой безопасности России, Федеральной службой по техническому и экспортному контролю России и другими министерствами и ведомствами.

1.8. Работа специалиста по информационной безопасности проводится в соответствии с планами работ.

На специалиста по информационной безопасности запрещается возлагать задачи, не связанные с его деятельностью.

1.9. В своей работе специалист по информационной безопасности руководствуется законодательными и иными нормативными актами Российской Федерации, Положением о государственной системе защиты информации в Российской Федерации от иностранных технических разведок и от ее утечки по техническим каналам, решениями Федеральной службы по техническому и экспортному контролю (Гостехкомиссии России), приказами и указаниям Министра и другими руководящими документами по защите информации и противодействию техническим средствам разведки.

II. Основные функции специалиста по информационной безопасности

2.1. Проведение единой технической политики, организация и координация работ по защите информации в Совете и Исполнительном комитете Сармановского муниципального района.

2.2. Осуществление планирования работ по защите информации от иностранных технических разведок и от ее утечки по техническим каналам.

2.3. Участие в подготовке объектов Совета и Исполнительного комитета Сармановского муниципального района к аттестации по выполнению требований обеспечения защиты информации при проведении работ со сведениями соответствующей степени секретности.

2.4. Разработка нормативно-методических документов по защите информации в Совете и Исполнительном комитете Сармановского муниципального района.

2.5. Разработка (самостоятельно или совместно с режимно-секретными или другими подразделениями) проектов распорядительных документов по вопросам организации защиты информации в Совете и Исполнительном комитете Сармановского муниципального района.

2.6. Организация в установленном порядке расследования причин и условий появления нарушений в области защиты информации и разработка предложений по устранению недостатков и предупреждению подобного рода нарушений, а также осуществление контроля за устранением этих нарушений.

2.7. Разработка предложений, участие в проводимых работах по совершенствованию системы защиты информации Совета и Исполнительного комитета Сармановского муниципального района.

2.8. Подготовка рекомендаций по перечню подведомственных предприятий, учреждений и организаций, которые подлежат лицензированию на право проведения мероприятий и (или) оказания услуг в области защиты информации.

2.9. Организация и координация разработки, внедрения и эксплуатации системы мер по безопасности информации, обрабатываемой техническими средствами в целях предотвращения утечки информации по техническим каналам.

2.10. Разработка (самостоятельно или совместно с режимно-секретными или другими подразделениями) комплекса мероприятий по защите информации при установлении и осуществлении научно-технических и торгово-экономических связей с зарубежными организациями, а также при посещении Совета и Исполнительного комитета Сармановского муниципального района или подведомственных предприятий, учреждений и организаций иностранными представителями.

2.11. Участие в согласовании технических заданий на проведение работ, содержащих сведения, отнесенные к государственной или служебной тайне.

2.12. Проведение периодического контроля эффективности мер защиты информации в Совете и Исполнительном комитете Сармановского муниципального района. Учет и анализ результатов контроля.

2.13. Организация повышения осведомленности по вопросам защиты информации руководства и сотрудников Совета и Исполнительного комитета Сармановского муниципального района, сотрудников подведомственных предприятий, учреждений и организаций.

2.14. Подготовка отчетов о состоянии работ по защите информации в Совете и Исполнительном комитете Сармановского муниципального района.

III. Права специалиста по информационной безопасности

Специалист по информационной безопасности имеет право:

3.1. Запрашивать и получать необходимые материалы для организации и проведения работ по вопросам защиты информации.

3.2. Разрабатывать проекты организационных и распорядительных документов по защите информации.

3.3. Готовить предложения о привлечении к проведению работ по защите информации на договорной основе организаций, имеющих лицензии на право проведения работ в области защиты информации.

3.4. Контролировать деятельность структурных подразделений Совета и Исполнительного комитета Сармановского муниципального района в части выполнения ими требований по защите информации.

3.5. Участвовать в работе постоянно действующей технической комиссии Совета и Исполнительного комитета Сармановского муниципального района при рассмотрении вопросов по защите информации.

3.6. Вносить предложения Главе о приостановке работ в случае обнаружения несанкционированного доступа, утечки (или предпосылок для утечки) информации, содержащей сведения, отнесенные к государственной или служебной тайне.

3.7. Привлекать в установленном порядке необходимых специалистов из числа сотрудников Совета и Исполнительного комитета Сармановского муниципального района для проведения исследований, разработки решений, мероприятий и организационно-распорядительных документов по вопросам защиты информации.

IV. Ответственность специалиста по информационной безопасности

4.1. Специалист по информационной безопасности несет персональную ответственность за:

соответствие визируемых им документов, представляемых на подпись руководству Совета и Исполнительного комитета Сармановского муниципального района;

правильность и объективность принимаемых решений;

правильное и своевременное выполнение приказов, распоряжений, указаний руководства Совета и Исполнительного комитета Сармановского муниципального района по вопросам, входящим в возложенные на него функции;

выполнение возложенных на него обязанностей, предусмотренных настоящим Положением;

соблюдение трудовой дисциплины, охраны труда;

реализацию принятой в Совете и Исполнительном комитете Сармановского муниципального района политики информационной безопасности.

качество проводимых работ по обеспечению защиты информации в соответствии с функциональными обязанностями.

согласно действующему законодательству российской Федерации за разглашение сведений, составляющих государственную, служебную или иную тайну, и сведений ограниченного распространения, ставших известными ему по роду работы.

Приложение 3
Для служебного пользования
Экз. № ___

УТВЕРЖДЕН
Постановлением Главы
Сармановского
муниципального района
от «09» марта 2016 г. №66

Регламент доступа в помещения с серверным и телекоммуникационным оборудованием

1. Помещения с серверным и телекоммуникационным оборудованием (далее – серверные помещения) Совета и Исполнительного комитета Сармановского муниципального района относятся к помещениям с ограниченным доступом.

2. К серверным помещениям Совета и Исполнительного комитета Сармановского муниципального района относятся помещения, где установлено серверное и телекоммуникационное оборудование Совета и Исполнительного комитета Сармановского муниципального района.

3. Серверные помещения должны быть оснащены охлаждающим оборудованием, средствами контроля доступа и охранной сигнализацией. Оснащение серверных помещений должно соответствовать правилам техники безопасности, санитарным нормам, отвечать требованиям пожарной безопасности, исключать возможность бесконтрольного проникновения в него посторонних лиц, гарантировать сохранность находящегося в нем имущества, работоспособность серверного и коммутационного оборудования.

4. Входные двери в серверные помещения должны быть прочными (рекомендуется установка металлических дверей) и должны быть оборудованы замками, гарантирующими надежное закрытие помещений в нерабочее время.

5. В серверные помещения допускаются лица, которые имеют прямое отношение к проводимым в этих помещениях работам, а также лица, осуществляющие контроль за проведение работ. Перечень таких лиц утверждается Постановлением Главы (Приложение 1 к настоящему регламенту). Доступ других лиц в серверное помещение может быть разрешен лишь в случае служебной необходимости руководителем аппарата Совета и фиксируется в «Журнале контроля допуска в серверное помещение» (Приложение 2 к настоящему регламенту) специалистом по информационной безопасности.

6. Все работы, проводимые на серверном или коммутационном оборудовании, хозяйственные, ремонтные работы, в том числе уборка могут проводиться лишь в присутствии лиц, указанных в Приложении 1 к настоящему Регламенту и фиксируются в «Журнале контроля допуска в серверное помещение» специалистом по информационной безопасности.

7. Серверные помещения должны быть в установленном порядке обеспечены первичными и исправными средствами пожаротушения и пожарной сигнализацией. Каждый сотрудник в соответствии с перечнем лиц, указанных в

Приложении 1 к настоящему Регламенту, обязан уметь пользоваться первичными средствами пожаротушения. Ответственный за противопожарное состояние серверных помещений Совета и Исполнительного комитета Сармановского муниципального района должен ежедневно проводить их осмотр, своевременно проверять годность огнетушителей.

8. При пожаре, аварии или стихийном бедствии сотрудник охраны (дежурный) Совета и Исполнительного комитета Сармановского муниципального района немедленно вызывает пожарную команду или аварийно-спасательную службу, ставит в известность ответственного за противопожарное состояние серверных помещений Совета и Исполнительного комитета Сармановского муниципального района, Главу. В случае чрезвычайных ситуаций коммутационные шкафы, отдельные серверы отсоединяются от сетей и выносятся из серверного помещения в безопасное место сотрудниками Совета и Исполнительного комитета Сармановского муниципального района совместно с сотрудниками охраны и аварийно-спасательных служб.

Приложение 1

УТВЕРЖДЕН
Постановлением Главы
Сармановского
муниципального района
от «09» марта 2016 г. №66

Список лиц допущенных в серверное помещение Министерства

№ п/п	ФИО	Должность	Отдел
1.	Андриянова Эльвира Ивановна	Главный специалист	Исполнительный комитет
2.	Сибгатуллин Ильнур Мунавирович	Системный администратор	Исполнительный комитет

Приложение 2

ЖУРНАЛ
УЧЕТА РАБОТ В СЕРВЕРНОМ ПОМЕЩЕНИИ КОМ. №____

Начат: «___»_____ ____ г.
Окончен: «___»_____ ____ г.
Срок хранения _____

Дата	Время входа / выхода	Ф.И.О. сотрудника, телефон	Наименование организации	Проведенные работы	Подпись сотрудника	Подпись ответственного за вход
1	2	3	4	5	6	7

Приложение 4
Для служебного пользования
Экз. № ___

УТВЕРЖДЕНА
Постановлением Главы
Сармановского
муниципального района
от «09» марта 2016 г. № 66

ИНСТРУКЦИЯ

по обеспечению безопасности информации Пользователя ИТ-инфраструктуры Совета и Исполнительного комитета Сармановского муниципального района

1. Общие положения

1.1 Пользователями ресурсов ИТ-инфраструктуры (далее – Пользователи) являются сотрудники Совета и Исполнительного комитета Сармановского муниципального района, прошедшие установленную процедуру регистрации в качестве Пользователей (получение учетной записи и пароля).

1.2. Положения Инструкции обязательны для исполнения всеми Пользователями.

1.3. Все Пользователи должны быть ознакомлены с данной Инструкцией и предупреждены о возможной ответственности за ее нарушение.

2. Обязанности пользователя

2.1. Пользователь ресурсов ИТ-инфраструктуры обязан:

- входить в сеть только под своим именем и паролем, полученными в ходе регистрации Пользователя ресурсов ИТ-инфраструктуры.
- использовать доступ к локальным и глобальным сетям только в профессиональных и служебных целях;
- исключить возможность неосторожного причинения вреда (действием или бездействием) техническим и информационным ресурсам ИТ-инфраструктуры;
- не предпринимать попыток несанкционированного доступа к информационным и вычислительным ресурсам локальных и глобальных сетей;
- перед использованием или открытием файлов, полученных из других источников, проверять файлы на наличие вирусов;
- не использовать доступ к сети для распространения и тиражирования информации, распространение которой преследуется по закону, заведомо ложной информации и информации, порочащей организации и физические лица, а также информации ограниченного пользования;
- производить блокировку рабочей станции при необходимости покинуть рабочее место;
- представлять свою рабочую станцию администратору безопасности для контроля;
- немедленно выполнять предписания администратора безопасности.

2.2. Пользователям ресурсов ИТ-инфраструктуры запрещено:

- открывать файлы и запускать программы на локальном компьютере из непроверенных источников или принесённых с собой на переносных носителях без предварительного сохранения на локальном жестком диске и последующей проверкой антивирусной программой;
- открывать на локальном компьютере приложения к почте из непроверенных источников без предварительного сохранения на локальном жестком диске и последующей проверкой антивирусной программой;
- хранение на файл-сервере файлов, не относящихся к выполнению служебных обязанностей сотрудника;

- фиксировать свои идентификационные реквизиты (пароли, идентификаторы и др.) на бумажных и других носителях;

- передавать посторонним свои идентификационные реквизиты (пароли, идентификаторы и др.);

- оставлять без присмотра или передавать посторонним свои смарт-карты и ключи электронной цифровой подписи;

- использовать неучтенные носители информации на АРМ;

- выносить с территории Совета и Исполнительного комитета Сармановского муниципального района и передавать третьим лицам носители информации.

3. Ответственность пользователя при работе в сети

3.1. Пользователь ресурсов ИТ-инфраструктуры несет персональную ответственность за соблюдение установленных требований во время работы в корпоративной локальной вычислительной сети.

3.2. Пользователи ресурсов ИТ-инфраструктуры, виновные в нарушении законодательства Российской Федерации о защите прав собственности и охраняемых по закону сведений, несут уголовную, административную, гражданско-правовую или дисциплинарную ответственность в соответствии с действующим законодательством и организационно-распорядительными документами Совета и Исполнительного комитета Сармановского муниципального района.

3.3. В случае причинения материального ущерба пользователь несет материальную ответственность в полном объеме и обязан возместить материальный ущерб.

Приложение 5
Для служебного пользования
Экз. № ___

УТВЕРЖДЕН
Постановлением Главы
Сармановского
муниципального района
от «09» марта 2016 г. №66

Положение о категорировании информационных ресурсов

1. Общие положения

1.1. Настоящим Положением о категорировании информационных ресурсов (далее Положение) вводятся категории информационных ресурсов и устанавливается порядок категорирования информационных ресурсов автоматизированных систем (далее АС) Совета и Исполнительного комитета Сармановского муниципального района, подлежащих защите.

Согласно Руководящему документу «Автоматизированные системы. Защита от несанкционированного доступа к информации. Классификация автоматизированных систем и требования по защите информации», утвержденному решением председателя Государственной технической комиссии при Президенте Российской Федерации от 30 марта 1992 года, для проведения классификации АС Совета и Исполнительного комитета Сармановского муниципального района необходимы следующие исходные данные:

- перечень защищаемых информационных ресурсов АС Совета и Исполнительного комитета Сармановского муниципального района, подлежащих защите и уровень их конфиденциальности;
- перечень лиц, имеющих доступ к штатным средствам АС, с указанием их уровня полномочий;
- матрица доступа или полномочий субъектов доступа по отношению к информационным ресурсам АС, подлежащих защите.

1.2. Категорирование информационных ресурсов АС является необходимым элементом организации работ по обеспечению информационной безопасности Совета и Исполнительного комитета Сармановского муниципального района и имеет своими целями:

- создание основы для классификации АС Совета и Исполнительного комитета Сармановского муниципального района;
- типизацию принимаемых организационных мер и распределения аппаратно-программных средств защиты информационных ресурсов по рабочим станциям (далее РС) и серверам АС Совета и Исполнительного комитета Сармановского муниципального района и унификацию вариантов настроек средств защиты.

2. Категории защищаемой информации

2.1. Исходя из необходимости обеспечения различных уровней защиты разных видов информации (не содержащей сведений, составляющих государственную тайну), хранимой и обрабатываемой в АС Совета и Исполнительного комитета Сармановского муниципального района, а также с учетом возможных путей нанесения ущерба Совету и Исполнительному комитету Сармановского муниципального района вводится три категории конфиденциальности защищаемой информации.

2.2. Категории конфиденциальности защищаемой информации:

- «Строго конфиденциальная» - к данной категории относится информация, являющаяся конфиденциальной в соответствии с требованиями действующего, а также информация, ограничения на распространение которой введены решениями руководства Совета и Исполнительного комитета Сармановского муниципального района, разглашение которой может привести к нанесению тяжкого ущерба Совету и Исполнительному комитету Сармановского муниципального района;
- «Конфиденциальная» - к данной категории относится информация, не отнесенная к категории «Строго конфиденциальная», ограничения на распространение которой вводятся решением руководства Совета и Исполнительного комитета Сармановского муниципального района в соответствии с предоставленными ему как собственнику либо уполномоченному собственником лицу информации действующим законодательством правами, разглашение которой может привести к нанесению ощутимого ущерба Совету и Исполнительному комитету Сармановского муниципального района;
- «Открытая» - к данной категории относится информация, обеспечения конфиденциальности которой не требуется.

2.3. Виды тайн:

- адвокатская тайна (Федеральный закон РФ «Об адвокатской деятельности и адвокатуре в Российской Федерации» от 31.05.2002 № 63-ФЗ);
- банковская тайна (Федеральный закон РФ «О банках и банковской деятельности» от 2 декабря 1990 г. № 395-1 (с изменениями от 29 июля 2004 г.));
- врачебная тайна («Основы законодательства Российской Федерации об охране здоровья граждан» от 22 июля 1993 г. № 5487-1 (с изменениями на 22 августа 2004 г.));
- персональные данные, личная и семейная тайна («Перечень сведений конфиденциального характера» (утвержден Указом Президента РФ от 6 марта 1997 г. № 188));
- служебная и коммерческая тайна («Перечень сведений конфиденциального характера»
(утвержден Указом Президента РФ от 6 марта 1997 г. № 188));
- тайна связи (Федеральный закон РФ «О связи» от 07.07.2003 № 126-ФЗ);
- тайна следствия и судопроизводства («Уголовно-процессуальный кодекс Российской Федерации» от 18.12.2001 № 174-ФЗ);
- тайна совещания судей («Уголовно-процессуальный кодекс Российской Федерации» от 18.12.2001 № 174-ФЗ).

3. Порядок определения категорий защищаемых информационных ресурсов АС

3.1. Категорирование информационных ресурсов АС проводится на основе их инвентаризации согласно методике категорирования защищаемых информационных ресурсов (Приложение 1 к настоящему Положению) и предполагает составление и последующее ведение, поддержание в актуальном состоянии перечня информационных ресурсов АС, подлежащих защите (Приложение 2 к настоящему Положению).

3.2. Ответственность за составление и ведение перечня информационных ресурсов АС, подлежащих защите (Приложение 2 к настоящему Положению), перечня лиц, имеющих доступ к штатным средствам АС (Приложение 3 к настоящему Положению), с указанием их уровня полномочий, и матрицы доступа или полномочий субъектов доступа по отношению к информационным ресурсам АС, подлежащим защите, (Приложение 4 к настоящему Положению) Совета и Исполнительного комитета Сармановского муниципального района возлагается:

- в части составления и ведения перечней и матрицы доступа - на специалиста по информационной безопасности;
- в части определения требований к обеспечению конфиденциальности и присвоение соответствующих категорий информационным ресурсам - на соответствующие отделы Совета и Исполнительного комитета Сармановского муниципального района, которые непосредственно работают с информационными ресурсами, и специалиста по информационной безопасности.

3.3. Контроль за правильностью категорирования информационных ресурсов АС Министерства осуществляется соответствующим специалистом по информационной безопасности Совета и Исполнительного комитета Сармановского муниципального района.

3.4. Категорирование информационных ресурсов АС Совета и Исполнительного комитета Сармановского муниципального района может осуществляться последовательно для каждой конкретной подсистемы АС в отдельности с последующим объединением и формированием единого перечня информационных ресурсов АС с Совета и Исполнительного комитета Сармановского муниципального района, подлежащих защите.

3.5. Изменение категории информационных ресурсов АС Совета и Исполнительного комитета Сармановского муниципального района производится при изменении требований к обеспечению защиты свойств конфиденциальности соответствующей информации.

3.6. Периодически (раз в год) или по требованию руководителей структурных подразделений Совета и Исполнительного комитета Сармановского муниципального района, использующих АС, производится пересмотр установленных категорий защищаемых информационных ресурсов АС Совета и Исполнительного комитета Сармановского муниципального района на предмет их соответствия реальному положению дел.

4. Порядок пересмотра положения

4.1. В случае внесения изменений и дополнений в перечень информационных ресурсов, подлежащих защите, пересмотру с последующим утверждением подлежит Приложение 2.

4.2. Любой пересмотр настоящего положения должен осуществляться на основании решения руководства Совета и Исполнительного комитета Сармановского муниципального района.

Приложение 1
к Положению о категорировании
информационных ресурсов

Методика категорирования защищаемых информационных ресурсов

1. Настоящая методика уточняет порядок проведения работ по категорированию информационных ресурсов АС Совета и Исполнительного комитета Сармановского муниципального района, подлежащих защите, в соответствии с Положением о категорировании информационных ресурсов.

2. Категорирование предполагает проведение работ по выявлению и анализу всех информационных ресурсов подсистем АС Совета и Исполнительного комитета Сармановского муниципального района, подлежащих защите.

3. Для проведения анализа всех подсистем АС Совета и Исполнительного комитета Сармановского муниципального района и проведения инвентаризации информационных ресурсов АС, подлежащих защите, формируется специальная рабочая группа. В состав этой группы включаются специалисты информационных технологий, информационной безопасности и других отделов Совета и Исполнительного комитета Сармановского муниципального района (осведомленные в вопросах технологии автоматизированной обработки информации в АС Совета и Исполнительного комитета Сармановского муниципального района). Для придания необходимого статуса рабочей группе, издается соответствующее распоряжение руководства Совета и Исполнительного комитета Сармановского муниципального района, в котором, в частности, даются указания всем начальникам структурных подразделений Совета и Исполнительного комитета Сармановского муниципального района об оказании содействия и необходимой помощи рабочей группе в проведении работ по анализу информационных ресурсов всех АС Совета и Исполнительного комитета Сармановского муниципального района. Для оказания помощи на время работы группы в подразделениях начальниками этих подразделений должны выделяться сотрудники, владеющие детальной информацией по вопросам обработки информации в данных подразделениях.

4.В ходе обследования конкретных подразделений Совета и Исполнительного комитета Сармановского муниципального района и автоматизированных подсистем выявляются все виды информационных ресурсов, используемых при решении задач в подразделениях Совета и Исполнительного комитета Сармановского муниципального района.

5.Все, выявленные в ходе обследования, информационные ресурсы заносятся в перечень информационных ресурсов, подлежащих защите (Приложение 2 к Положению о категорировании информационных ресурсов).

6.Далее определяется и затем указывается в перечне информационных ресурсов, подлежащих защите, категория конфиденциальности и к какому типу тайны относится каждый из выявленных информационных ресурсов на основании требований действующего законодательства и предоставляемых Совету и Исполнительному комитету Сармановского муниципального района прав.

7.Первоначальные предложения по оценке категорий обеспечения конфиденциальности конкретных видов информации выясняются у руководителей соответствующих структурных подразделений Совета и Исполнительного комитета Сармановского муниципального района. Данные оценки категорий информации заносятся в перечень информационных ресурсов, подлежащих защите (в колонку 2). Размещение информационного ресурса АС Совета и Исполнительного комитета Сармановского муниципального района выясняется у соответствующего сотрудника информационных технологий Совета и Исполнительного комитета Сармановского муниципального района.

8.В дальнейшем, с участием специалистов информационных технологий и информационной безопасности Совета и Исполнительного комитета Сармановского муниципального района необходимо уточнить и внести в Приложение 3 к Положению о категорировании информационных ресурсов сведения о пользователях и их уровне доступа к штатным средствам АС Совета и Исполнительного комитета Сармановского муниципального района.

9.Затем Перечень лиц, имеющих доступ к штатным средствам АС, согласовывается с руководителями Совета и Исполнительного комитета Сармановского муниципального района и утверждается Главой.

10.На следующем этапе составляется матрица доступа или полномочий субъектов доступа по отношению информационным ресурсам АС, подлежащим защите (Приложение 4 к Положению о категорировании информационных ресурсов).

11.На последнем этапе определяется класс АС на основании руководящего документа «Автоматизированные системы. Защита от несанкционированного доступа к информации. Классификация автоматизированных систем и требования по защите информации». Исходя из класса АС определяются типовые конфигурации принимаемых мер и настройки защитных механизмов программно-аппаратных средств защиты информации.

Приложение 2
к Положению о категорировании
информационных ресурсов

Для служебного пользования
Экз. № ___

ПЕРЕЧЕНЬ* ИНФОРМАЦИОННЫХ РЕСУРСОВ АС МИНИСТЕРСТВА, ПОДЛЕЖАЩИХ ЗАЩИТЕ

№ п/п	Наименование информационного ресурса (информации)	Категория конфиденциальности и вид тайны	Размещение ресурса (РС, устройство, каталог, файл)	Ответственный (подразделение) за определение требований к защищенности ресурса
1.	1С	Строго конфиденциальная, персональные данные	РС	Отдел бухгалтерского учета и отчетности

Приложение 3
к Положению о категорировании
информационных ресурсов

Для служебного пользования
Экз. № ___

ПЕРЕЧЕНЬ* ЛИЦ, ИМЕЮЩИХ ДОСТУП К ШТАТНЫМ СРЕДСТВАМ АС.

№ п/п	Наименование штатных средств	ФИО, должность лица, имеющего доступ	Уровень доступа к штатным средствам
1.			
2.			
3.			

Приложение 4

к Положению о категорировании
информационных ресурсов

МАТРИЦА ДОСТУПА ИЛИ ПОЛНОМОЧИЙ СУБЪЕКТОВ ДОСТУПА ПО ОТНОШЕНИЮ К ИНФОРМАЦИОННЫМ РЕСУРСАМ АС, ПОДЛЕЖАЩИМ ЗАЩИТЕ.

№ п/п	Помещение (каб.№)	АРМ №	Имя АРМ в домене tatar.ru	IP адрес	Имя пользователя	Подсистемы/ Задачи	Ф.И.О. пользователя	Категория доступа	Номер пункта из Перечня	Подразделение
1										

Приложение 6
Для служебного пользования
Экз. № ___

УТВЕРЖДЕН
Постановлением Главы
Сармановского
муниципального района
от «09» марта 2016 г.
№ 66

СОГЛАСИЕ
работника на обработку персональных данных

Я, нижеподписавшийся _____,
(Ф.И.О. полностью)
зарегистрированный по адресу: _____
_____,
проживающий по адресу: _____,
документ, удостоверяющий личность паспорт серия _____ номер _____,
выдан _____
(дата и название выдавшего органа)
_____
своей волей и в своем интересе подтверждаю свое согласие на обработку Советом и Исполнительным комитетом Сармановского муниципального района Республики Татарстан, расположенным по адресу: 423350, Республика Татарстан, Сармановский район, с.Сарманово, ул.Ленина, д.35, моих персональных данных.

Цель обработки персональных данных: в соответствии с требованиями ст.ст. 23, 24 Конституции РФ, статьи 9 Федерального закона от 27.07.06 г. № 152-ФЗ «О персональных данных», на основании ст. 86-90 Трудового Кодекса Российской Федерации, Федеральным законом от 27 июля 2004 г. №79-ФЗ «О государственной гражданской службе Российской Федерации», в целях обеспечения соблюдения законодательства Российской Федерации в области персональных данных и иных нормативных правовых актов с учетом положений Федерального закона № 152-ФЗ «О персональных данных», оформления трудовых отношений, расчета и выдачи заработной платы или других доходов, налоговых и пенсионных отчислений, содействия работникам в трудоустройстве, обучении, повышении квалификации и продвижении по службе, обеспечения личной безопасности работников, контроля количества и качества выполняемой работы, обеспечения сохранности имущества работодателя в соответствии с законодательством Российской Федерации в области персональных данных.

Перечень персональных данных, на обработку которых дано настоящее согласие:
- фамилия, имя, отчество;
- паспортные данные (+ ксерокопия паспорта);
- дата и место рождения;
- пол;
- гражданство;
- адрес места жительства (по паспорту, фактический);
- сведения о воинском учете;
- семейное положение;
- сведения о составе семьи;
- стаж работы;
- контактный номер телефона;

- сведения об образовании;
- профессия (специальность);
- должность;
- сведения об аттестации;
- сведения о повышении квалификации;
- сведения о профессиональной переподготовки;
- сведения о наградах (поощрениях), почетных званиях;
- сведения о социальных льготах;
- сведения о заработной плате;
- номер лицевого (расчетного) счета;
- сведения, содержащиеся в трудовой книжке;
- сведения, содержащиеся в свидетельстве о постановке на учет в налоговом органе (ИНН);
- сведения, содержащиеся в страховом свидетельстве государственного пенсионного страхования (СНИЛС).

Перечень действий с персональными данными, на совершение которых дается согласие: обработка персональных данных, включая сбор, запись, систематизацию, накопление, хранение, уточнение (обновление, изменение), извлечение, использование, передачу (распространение, предоставление, доступ), обезличивание, блокирование, удаление, уничтожение персональных данных.

Если распространение (в том числе передача) информации о персональных данных производится в не предусмотренных Федеральным законодательством случаях обязательного предоставления субъектом персональных данных своих персональных данных, работодатель (оператор) обязан запросить письменное согласие работника в каждом отдельном случае.

Способы обработки персональных данных: на бумажных носителях; в информационных системах персональных данных с использованием и без использования средств автоматизации, а также смешанным способом; при участии и при непосредственном участии человека.

Срок, в течение которого действует согласие: до достижения цели обработки персональных данных или до момента утраты необходимости в их достижении, если иное не предусмотрено Федеральным законодательством.

Настоящее согласие может быть отозвано мной путем подачи в Совет и Исполнительный комитет Сармановского муниципального района Республики Татарстан письменного заявления об отзыве согласия.

Подтверждаю, что я ознакомлен с Положением о защите персональных данных муниципального служащего Совета и Исполнительного комитета Сармановского муниципального района Республики Татарстан, права и обязанности в области защиты персональных данных мне разъяснены.

«___» _____ 20___ г. _____ _____

(подпись) (расшифровка подписи работника)