МИНИСТЕРСТВО ФИНАНСОВ РЕСПУБЛИКИ ТАТАРСТАН

ТАТАРСТАН РЕСПУБЛИКАСЫ ФИНАНС МИНИСТРЛЫГЫ

ПРИКАЗ

БОЕРЫК

25.10.2013 № 21-21-54

г. Казань

В целях создания условий для повышения информационной безопасности в Министерстве финансов Республики Татарстан п р и к а з ы в а ю:

1. Утвердить «Политику информационной безопасности Министерства финансов Республики Татарстан» согласно приложению.

2. Начальнику отдела кадров Министерства финансов Республики Татарстан и начальнику отдела кадров Департамента казначейства Министерства финансов Республики Татарстан обеспечить ознакомление государственных служащих с политикой информационной безопасности при заключении служебных контрактов.

3. Начальнику отдела методологии проектов, начальнику отдела технического обеспечения и начальнику отдела режима секретности и безопасности Департамента казначейства Министерства финансов Республики Татарстан обеспечить проведение с сотрудниками Министерства финансов Республики Татарстан и Департамента казначейства Министерства финансов Республики Татарстан инструктажей по обеспечению режима информационной безопасности в объёме, необходимом для выполнения ими своих служебных обязанностей.

4. Сотрудникам Министерства финансов Республики Татарстан при выполнении своих должностных обязанностей руководствоваться «Политикой информационной безопасности Министерства финансов Республики Татарстан», утверждённой настоящим приказом.

5. Контроль за выполнением настоящего приказа оставляю за собой.

Министр Р.Р.Гайзатуллин

Приложение
к приказу
Министерства финансов
Республики Татарстан
от 25.10.2013г № 21-21-54

Политика информационной безопасности.

1. Общие положения.

1.1. Министерство финансов Республики Татарстан (далее – Министерство) является исполнительным органом государственной власти Республики Татарстан, обеспечивающим проведение единой финансовой, бюджетной, налоговой политики в Республике Татарстан и координирует деятельность в этой сфере иных органов исполнительной власти Республики Татарстан. Осуществление указанной деятельности связано с управлением информацией, являющейся важным активом Министерства, и зависит от обеспечения информационной безопасности, под которой понимается обеспечение конфиденциальности, целостности и доступности информационных активов.

1.2. Политика информационной безопасности Министерства (далее – Политика ИБ) устанавливает цели, задачи и подходы в области информационной безопасности, которыми Министерство руководствуется в своей деятельности.

1.3. Принимаемые меры защиты информации должны 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) Министерства независимо от типа носителя этих данных.

1.4. Положения и требования Политики ИБ распространяются на всех сотрудников Министерства, а также основных разработчиков и исполнителей, которые участвуют в разработке, создании, развертывании, вводе в эксплуатацию и использовании информационных систем, в пределах их компетенции.

1.5. Политика ИБ является методологической основой для:

- разработки подсистемы информационной безопасности при доступе к информации, реализуемой на объектах информатизации с ограниченным доступом, в виде комплексной системы защиты информации от несанкционированного доступа;
- разработки защищенного электронного документооборота, с использованием средств криптографической защиты информации, применения электронной цифровой подписи при обмене защищаемой информацией;
- разработки конкретных нормативных документов регламентирующих деятельность в области обеспечения информационной безопасности и при проведении соответствующих мероприятий;
- реализации прав граждан, организаций и государства на получение, распространение и использование информации.

Настоящая Политика ИБ разработана на основе требований действующих в Российской Федерации законодательных и нормативных документов, регламентирующих вопросы защиты информации. Основными документами, используемыми при разработке Политики ИБ являются:

- Закон Российской Федерации от 21 июля 1993 г. № 5485-1 «О государственной тайне»;
- Федеральный закон от 29 июля 2004 г. № 98-ФЗ «О коммерческой тайне»;
- Федеральный закон от 27 июля 2006 г. № 149-ФЗ «Об информации, информационных технологиях и о защите информации»;
- Федеральный закон от 27 июля 2006 г. № 152-ФЗ «О персональных данных»;
- Указ Президента Российской Федерации от 06.03.1997 г. № 188 «Об утверждении перечня сведений конфиденциального характера»;
- Приказ Государственной технической комиссии при Президенте Российской Федерации от 30 августа 2002 г. № 282 «Об утверждении «Специальных требований и рекомендаций по технической защите конфиденциальной информации»;
- ГОСТ Р ИСО/МЭК 17799-2005 «Информационная технология. Практические правила управления информационной безопасностью», утвержденный приказом Министерства промышленности и энергетики

Российской Федерации, Федерального агентства по техническому регулированию и метрологии от 29.12.2005г. № 447-ст «Об утверждении национального стандарта»;

- ГОСТ Р ИСО/МЭК 15408-1-2008 «Информационная технология. Методы и средства обеспечения безопасности. Критерии оценки безопасности информационных технологий», утвержденный приказом Министерства промышленности и торговли Российской Федерации, Федерального агентства по техническому регулированию и метрологии от 18.12.2008г. № 519-ст «Об утверждении национального стандарта».

2. Цель обеспечения информационной безопасности

Политика ИБ направлена на достижение следующих целей:

- обеспечение непрерывности решения задач стоящих перед МФ РТ;
- минимизация возможных потерь и ущерба от нарушений в области информационной безопасности.

3. Объекты информационной безопасности МФ РТ

Основными объектами защиты Министерства являются:

- информационные ресурсы Министерства, содержащие сведения с персональными данными;
- информационные ресурсы, содержащие сведения, отнесенные к государственной тайне;
- информационные ресурсы Министерства ограниченного распространения, в том числе содержащие конфиденциальные сведения;
- программные информационные ресурсы Министерства, а именно: прикладное программное обеспечение, системное программное обеспечение, инструментальные средства и утилиты;
- физические информационные ресурсы Министерства: компьютерное аппаратное обеспечение всех видов; носители информации всех видов;
- технические сервисы Министерства (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. Их доступность, целостность и конфиденциальность имеют особое значение для обеспечения деятельности Министерства, эффективности его функционирования и т.д. Доступность, целостность и конфиденциальность информации в обязательном порядке учитывается при разработке организационно-распорядительной документации Министерства 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 Министерства являются:

- инвентаризация и систематизация всех информационных ресурсов Министерства;
- обеспечение безопасности информационных ресурсов Министерства: 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 и эффективной работы сотрудников Министерства с его информационными ресурсами;
- сведение к обоснованному минимуму финансовых затрат на поддержание функционирования на необходимом уровне аппаратного и программного обеспечения и автоматизированной системы в целом (сюда относятся крупные и мелкие обновления программного и аппаратного обеспечения, бесперебойное обеспечение системы).

5. Принципы обеспечения информационной безопасности Министерства.

Построение системы защиты информации в Министерстве основывается на следующих принципах:

- применение разнородных систем обеспечения информационной безопасности;

- преимущества одних частей системы обеспечения информационной безопасности должны перекрывать недостатки других;
- система обеспечения информационной безопасности должна быть 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 сотрудников Министерства.

6. Оценка рисков

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

- ущерб, который может нанести деятельности Министерства нарушение информационной безопасности, с учетом возможных последствий нарушения конфиденциальности, целостности и доступности информации;
- реальная вероятность нарушения защиты в свете превалирующих угроз и средств контроля.

7. Требования к обучению вопросам информационной безопасности

Основной целью обучения является:

- ознакомление сотрудников Министерства с угрозами и проблемами, связанными с информационной безопасностью и их ответственности в соответствии с законодательством. Доведение требований указанных документов до лиц, допущенных к защищаемой информации, должно осуществляться под роспись;

- обучение всех сотрудников Министерства правилам использования средств обработки информации, применяемыми на их рабочих местах, до предоставления доступа к информации или услугам.

Сотрудники Министерства должны знать и выполнять требования организационно-распорядительных документов Министерства в области информационной безопасности, касающиеся организации работ на их рабочих местах, а также требованиям к обеспечению безопасности обработки информации на средствах вычислительной техники и правилам работы в сети Интернет.

Если сотрудник работает со средствами защиты информации, то администратор безопасности данного объекта совместно с сотрудниками отдела режима секретности и безопасности Департамента казначейства Министерства финансов Республики Татарстан должны обучить сотрудника правильному использованию средств защиты информации, чтобы свести к минимуму возможные риски безопасности.

8. Управление информационной безопасностью

8.1. Для достижения целей обеспечения информационной безопасности в Министерстве создаётся система управления информационной безопасностью, которая соответствует законодательству Российской Федерации об информационной безопасности (далее – СИБ).

8.2. При разработке СИБ правила работы для каждого объекта защиты документируются в процедурах, рабочих инструкциях и правилах, определяющих обязанности пользователей систем и администраторов, которые являются обязательными для всех сотрудников Министерства.

8.3. Все информационные активы Министерства, включая аппаратное обеспечение, программное обеспечение, информационные ресурсы на бумажных и электронных носителях, подлежат учёту и категорированию в соответствии с их важностью и конфиденциальностью.

8.4. Выбор средств для защиты информации, включая организационные, физические, технические программные и программно – аппаратные, проводится на основании требований законодательства и оценки рисков информационной безопасности.

8.5. Для обеспечения физической защиты информационных активов в контролируемых зонах Министерства и его подразделений устанавливаются зоны с ограниченным доступом и принимаются меры для предотвращения неавторизованного доступа.

8.6. Министерство выявляет, учитывает и реагирует на инциденты в сфере информационной безопасности в соответствии с установленными процедурами.

8.7. В Министерстве разрабатываются процедуры, обеспечивающие непрерывность функционирования информационных систем при сбоях оборудования и технических неисправностях инженерных коммуникаций.

9. Ответственность.

9.1. Председатель постоянно действующей технической комиссии осуществляет общее управление информационной безопасностью и обеспечивает необходимые условия для создания СИБ и регулярного обучения сотрудников Министерства в сфере информационной безопасности.

9.2. Руководители структурных подразделений Министерства отвечают за выполнение в сфере своей компетенции положений и других внутренних документов Министерства, регламентирующих обеспечение информационной безопасности в их подразделениях, а также за формирование требований на подключение своих сотрудников к информационным ресурсам, обеспечивающим получение ими только необходимой информации.

9.3. Руководители структурных подразделений Министерства, работающие с информацией ограниченного доступа, несут персональную ответственность за сохранность информации на съёмных машинных носителях и на бумажных носителях, а также обеспечивают контроль за работой сотрудников подразделений, работающих с такой информацией.

9.4. Администраторы информационных систем обеспечивают их эффективное функционирование и отвечают за реализацию технических и организационных мер по конкретным информационным системам, за конкретное применение штатных механизмов защиты системных и информационных ресурсов, за доступ сотрудников только к той информации, которая определена как необходимая в требованиях, сформированных руководителем структурного подразделения сотрудника.

9.5. Сотрудники несут персональную ответственность за свои действия при обращении с информацией и при работе в информационных системах, а также за неразглашение паролей, сохранность электронных ключей и выполнение требований внутренних документов Министерства.

9.6. Административно - хозяйственный отдел Министерства и

административно – хозяйственный отдел Департамента казначейства Министерства финансов Республики Татарстан осуществляют обеспечение бесперебойной работы систем жизнеобеспечения, в том числе работоспособности систем электропитания, кондиционирования, противопожарной и охранной сигнализации на закреплённых за ними территориях.

Организацию технической защиты информации на электронных носителях осуществляют следующие отделы Департамента казначейства Министерства финансов Республики Татарстан:

- методологии проектов;
- технического обеспечения;
- режима секретности и безопасности.

Отдел режима секретности и безопасности несёт ответственность за:

- определение методологии построения системы безопасности объекта информатизации;
- выбор средств защиты,
- организацию, разработку и внедрение процедур, рабочих инструкций и правил, необходимых для обеспечения выбранных режимов защиты;
- подбор администраторов безопасности, осуществляющих контроль эффективности системы защиты Министерства.

Отдел методологии проектов несёт ответственность за:

- создание и ввод в эксплуатацию информационных систем;
- управление доступом к информационным ресурсам;
- обеспечение целостности и неизменности программного обеспечения и данных, регулярное резервное копирование информационных ресурсов;
- администрирование систем построения защищенных каналов, используя открытые каналы связи.
- Отдел технического обеспечения несёт ответственность за:
- организацию доступа пользователей только к необходимым им ресурсам;
- организацию антивирусной защиты;
- организацию доступа в информационно-телекоммуникационную сеть «Интернет»;
- работоспособность серверов, компьютеров, принтеров и другого оборудования необходимого для обработки информации;

- учёт материальных ресурсов и обеспечение своевременного восстановление их при неисправностях.

При разработке новых информационных систем отдел методологии проектов и отдел технического обеспечения Департамента казначейства Министерства финансов Республики Татарстан осуществляют разработку проектов объектов информатизации и их эксплуатацию только с учетом требований по защите информации, формируемых отделом режима секретности и безопасности Департамента казначейства Министерства финансов Республики Татарстан.

10.Заключительные положения

10.1. В случае изменения законодательных и (или) иных нормативных актов, в том числе Положения о Министерстве настоящая Политика ИБ и изменения к ней применяются в части, не противоречащей вновь принятым изменениям.

10.2. Внесение изменений в настоящую Политику ИБ осуществляется в случаях перечисленных в п.10.1., также по результатам анализа инцидентов информационной безопасности, актуальности, достаточности и эффективности используемых мер обеспечения информационной безопасности, результатам проведения внутренних аудитов информационной безопасности и других контрольных мероприятий.

10.3 Ответственным за внесение изменений в настоящую Политику является заместитель директора Департамента казначейства Министерства финансов Республики Татарстан, курирующий отдел режима секретности и безопасности.